08.2022 - São Paulo

Política de Segurança da Informação e Proteção de Dados

- **ÍNDICE**

• REGISTRO DE MUDANÇAS

Data	Autor	Aprovador	Versão	Referência de Mudança
11/08/2020	Esteban Huerta	Fernando Venega	1.0	Versão Inicial
08/03/2022	Esteban Huerta	Fernando Venega	1.1	Adequação LGPD
22/08/2022	Mateus Almeida	Fernando Venega	2.0	Adequação LGPD

Figura 1 - Registro de Mudanças

- **DEFINIÇÕES GERAIS**

1. INTRODUÇÃO

A BlueShift tem como fator primordial a ética e relações transparentes, assim como proíbe a prática de toda forma de corrupção, fraude, suborno, favorecimento e extorsão por seus colaboradores.

O objetivo deste documento é estabelecer regras e orientações bases para a utilização segura e ética dos recursos tecnológicos como diretrizes corporativas da BLUESHIFT BRASIL LTDA, inscrita no CNPJ sob número 15.549.414/0001-41, conforme regulamentado na Lei Geral de Proteção de Dados – LGPD (Lei Nº 13.709/2018), visando a proteção dos dados pessoais de base de clientes, colaboradores e demais envolvidos, como também assegurar a minimização de riscos do negócio.

A política aqui estabelecida deve ser cumprida por todas as partes envolvidas nas atividades vinculadas a BlueShift. É um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos os seus funcionários, colaboradores, consultores, parceiros, prestadores de serviços que venham ter acesso a dados pessoais e/ou recursos tecnológicos da BlueShift. Esta política estabelecida, dá ciência que tais acessos poderão ser monitorados com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

2. CONCEITOS BÁSICOS

Para efeitos de entendimento e fácil compreensão da política ora criada neste instrumento, serão apresentados as definições legais e conceitos que serão utilizados no decorrer deste documento;

a. **PSI:** Abreviação para Política de Segurança da Informação, que é um conjunto de padrões, normas e diretrizes a todos os colaboradores que utilizam infraestrutura computacional e/ou recursos tecnológicos da empresa. Ela tem como objetivo garantir a proteção das informações corporativas contra eventuais ameaças que possam prejudicar sua operação;

b. **Dados:** Parte elementar da estrutura do conhecimento incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis. Representa uma ação não descrita, uma quantidade sem especificar o objeto, por exemplo, dentro da LGPD temos os seguintes tipos de categorização de dados:

- **Dados pessoais:** São todos os tipos de dados que podem levar a identificação de uma pessoa, de forma direta ou indireta. Alguns tipos de dados pessoais incluem (nome completo, RG e CPF, passaporte e carteira de habilitação, endereço, telefone, e-mail, endereço de IP, data de nascimento, localização via GPS, entre outros);

- **Dados sensíveis:** Qualquer informação que relacione com a origem racial, étnica, credo, opinião política, filiação a sindicato; que se referem à saúde ou vida sexual, dados genéticos e biométricos;

- **Dados anonimizados:** São dados que passam por etapas que desvinculam qualquer possibilidade de identificação de seu titular;

- **Dados públicos:** São dados que devem ser tratados considerando a finalidade, a boa fé e o interesse público que justifiquem a sua disponibilização; tais dados merecem um estudo mais detalhado pois são dados que ainda públicos podem ser restringidos pelo indivíduo dependendo da forma, tratamento e/ou compartilhamento (§§ 3º e 4º do art. 7º da LGPD)

c. **ANPD – Autoridade Nacional de Proteção de Dados:** Órgão da administração pública direta federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil;
d. **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
e. **Controlador:** Pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais;
f. **Operador:** Pessoa natural ou jurídica, a quem realiza o tratamento de dados pessoais em nome do controlador;
g. **Suboperador:** Ainda que não previsto expressamente na LGPD, o Suboperador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em

nome do controlador, sendo, portanto, essencial na compreensão das operações de dados complexas como as que a BlueShift está inserida;

h. **Encarregado de dados:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (art. 5º, inciso VII da LGPD);
i. **Tratamento de dados:** Qualquer operação que seja realizada com os dados pessoais (incluindo: acesso, armazenamento, arquivamento, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização);
j. **Cliente:** Pessoa natural ou jurídica que contrate os serviços da BlueShift, ou que estejam em vias de contratar serviços;
k. **Colaborador:** Prestador de serviços diretos ou indiretos ativos junto a BlueShift;
l. **Parceiro/Prestador:** Pessoa natural ou jurídica que presta serviços a BlueShift no âmbito das atividades;
m. **Recursos tecnológicos:** São todos os recursos físicos e digitais utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar informações. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanner, entre outros;
n. **Dispositivo móvel:** Entende-se qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, smartphones, tablets entre outros;
o. **Incidentes de segurança da informação:** Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à esta política, a LGPD, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação. São exemplos de Incidentes de Segurança da Informação:

    I. Perda de serviços ou recurso;
    II. Mau funcionamento ou sobrecarga de sistema;
    III. Erros humanos;
    IV. Não conformidade com a Política e a Norma;
    V. Observações ou suspeitas de fragilidade em sistemas ou serviços;
    VI. Vazamento de informação de clientes ou pessoas físicas que estejam armazenadas e/ou tratadas em nosso ambiente digital;
    VII. Violações de procedimentos de segurança e violações de acesso.

p. **LGPD – Lei Geral de Proteção de Dados**: Lei de nº 13.709/2018 que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

q. **Criptografia:** É a conversão de dados de um formato legível em um formato codificado, tornando esses dados ilegíveis àqueles que não possuem o código correto para lê-los.

3. COMO A BLUESHIFT COLETA E QUAIS TIPOS DE DADOS TRATAMOS.

A BlueShift enquanto consultoria em tecnologia da informação especializada na criação e implementação de soluções em Big Data, Analytics, RPA e IoT, realiza o tratamento de diferentes tipos de dados em distintos contextos, com a comum finalidade de atender as necessidades de seus clientes e parceiros.

Nesse sentido, a coleta de dados realizada pela BlueShift se dá principalmente através da disponibilização de conjuntos de dados pelos clientes finais.

A avaliação dos tipos de dados a serem processados por meio das soluções e serviços oferecidos pela BlueShift é parte essencial e inicial do processo de contratação da BlueShift junto a seus clientes e parceiros, antecedendo as efetivas operações de processamento.

Com a finalidade de assegurar que somente serão disponibilizados para tratamento dados e conjuntos de dados que sejam coletados conforme os fundamentos e requisitos da LGPD, enunciados em seu Art. 7, a BlueShift firma junto a todos os seus clientes e parceiros o compromisso contratual de que este cumprimento dos requisitos anteceda qualquer operação de tratamento.

Após a verificação do cumprimento dos requisitos dos dados disponibilizados para tratamento, podemos realizar operações com diferentes categorias de dados, os quais listamos as seguintes, também com referência na LGPD:

- Dado pessoal
- Dado pessoal sensível
- Dado anonimizado
- Banco de dados

Também realizamos a coleta de dados de nossos colaboradores e candidatos em processo seletivo com distintas finalidades, as quais listamos algumas das hipóteses a seguir:

- Solicitação de informações necessárias para identificação durante o processo seletivo;
- Cumprir com os requisitos legais de contratação e criação dos contratos;
- Realizar o cadastro interno nas plataformas, ferramentas e recursos os quais o colaborador necessita de acesso para executar as atividades;

- Realizar o credenciamento e a homologação do acesso do colaborador junto aos clientes finais;
- Realização de ações positivas de gerenciamento de recursos humanos com a finalidade de promover o bem-estar, saúde e melhoria contínua do ambiente e das relações de trabalho de nossos colaboradores.

Ao acessar nosso site institucional via web, também é possível que sejam coletados dados de forma automática através de cookies, neste caso, o usuário será avisado imediatamente ao acesso do site sobre o aceite, gerenciamento dos cookies ou recusa da coleta de informações, tais como: dispositivo utilizado para o acesso, dados sobre a sessão, endereço IP, o navegador Web utilizado, o site de referência, data e horário do acesso, como também poderá acessar nossa política de cookies para melhor entendimento e detalhamento.

A BlueShift na hipótese de gerenciamento e administração de informações disponibilizadas é **controladora de dados**, promovendo ações positivas e negativas com em favor da proteção da privacidade, entre as quais citamos:

- Eliminação de dados fornecidos por participantes em processos seletivos após 90 dias do encerramento do processo;
- Eliminação de dados os quais a retenção não seja exigida legalmente após 90 dias a partir do fim da prestação de serviços;
- Anonimização da visualização de respostas a formulários gerados pelas ações de recursos humanos;
- Limitação do acesso aos dados apenas a pessoas que tenham autorização e extrema necessidade de acesso para a execução de suas atividades.

4. A BLUESHIFT ENQUANTO OPERADORA DE DADOS

Em nossas atividades junto aos clientes e parceiros, realizamos o processamento de dados sob a função de **operadora de dados**.

Nessa hipótese, em decorrência da diversidade de mercados os quais atuamos através de nossos clientes, os tipos de dados os quais temos acesso e realizamos atividades de processamento também é

diversificado. A título exemplificativo, destacamos alguns desses tipos, que podem ser pessoais ou não, como:

- Numéricos (exatos ou aproximados);
- Data, hora;
- Cadeias de caracteres, texto (estruturados ou não);
- Áudio;
- Vídeo

Enquanto operadores de dados, contamos com estrutura organizacional voltada a gestão eficaz de projetos através do diálogo e recebimento de instruções diretas por parte dos clientes. Dessa forma, a BlueShift realiza as atividades conforme instruções e definições do controlador de dados, atuando sempre conforme as seguintes finalidades:

- Entrega de serviços ou produtos contratados;
    - As operações de tratamento de dados são parte central das atividades da BlueShift, dessa forma, para cumprir com nossas obrigações firmadas, realizamos diferentes formas de tratamento, sendo os principais presentes no desenvolvimento de projetos e gerenciamento interno;
- Publicidade e alcance de novos clientes
    - A BlueShift realiza ações de publicidade/marketing, com o intuito de promover sua marca através de diferentes meios de comunicação;
- Para o cumprimento de obrigação legal, judicial ou regulatória;
    - A BlueShift respeita toda legislação e obrigações judiciais que regulam o tratamento dos dados em âmbito nacional, não se limitando a observação da LGPD e do GDPR. Dessa forma, também em respeito a outras legislações, realizamos o tratamento de dados quando exigido, com finalidades tais como a verificação de identidade, o cumprimento de leis trabalhistas e tributárias, entre outras disposições legais e judiciais;

5. COLABORADORES DA BLUESHIFT ENQUANTO SUBOPERADORES DE DADOS

Os consultores BlueShift, enquanto contratados para o apoio e desenvolvimento de projetos em nossos clientes, atuam como **suboperadores de dados**, realizando as atividades de tratamento de dados conforme orientação dos gestores de projeto e líderes técnicos, que em diálogo direto com os clientes, conduzem as atividades de acordo com as instruções do controlador de dados.

Em nosso processo de onboarding de colaboradores validamos o conhecimento sobre práticas anticorrupção e lavagem de dinheiro. Após este check inicial, solicitamos acesso ao ambiente cloud (da subscrição do cliente) ou ao ambiente de desenvolvimento on-premisses (provido pelo cliente) ao time alocado ao projeto e com direitos de acesso conforme requisitos do escopo de desenvolvimento.

Nossos consultores ao ingressar e durante todo o período de prestação de serviços, são treinados sobre práticas de desenvolvimento seguro, segurança da informação, práticas anticorrupção, lavagem de dinheiro e sigilo das informações.

O acesso físico e lógico ao final das atividades ou se houver desligamento é retirado previamente, evitando eventuais riscos de vazamento ou utilização indevida das informações as quais o colaborador tem acesso.

6. COMPARTILHAMENTO DE DADOS

A BlueShift, com exceção das hipóteses abaixo elencadas, não realiza o compartilhamento de dados de seus clientes, fornecedores, parceiros e colaboradores:

- Quando for necessário atender às obrigações legais ou regulatórias;
- Para cumprir com suas obrigações em contratos de prestação de serviço;
- Quando há justificativa e consentimento do titular de dados;
- Para o desenvolvimento das atividades de tratamento de dados através dos nossos colaboradores conforme a finalidade disposta pelo controlador.

7. DIREITOS DOS TITULARES DE DADOS

O titular dos dados possui o direito de saber exatamente como os dados são tratados, quais dados são coletados e o porquê e com quem eles são compartilhados.

Para além disso, a LGPD, em seu artigo 18, esclarece que o titular de dados possui 9 (nove) direitos principais tais como:

- Confirmação sobre a existência de operações de tratamentos sobre dados pessoais;
- Acesso aos dados pessoais que a BlueShift possui em seus arquivos;
- Correção sobre dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação

  O titular dos dados pode solicitar (a) a anonimização dos seus Dados Pessoais (b) o bloqueio dos seus Dados Pessoais, suspendendo operações de tratamento e (c) a eliminação dos seus Dados Pessoais, caso em que deveremos apagar todos os seus Dados Pessoais, com ressalva dos dados que precisam ser mantidos para cumprimento de obrigações legais e/ou contratuais por parte da BlueShift;

- Portabilidade

  O titular pode solicitar o fornecimento de seus dados pessoais de forma estruturada e interoperável visando à sua transferência para um terceiro, não incluindo dados que já tenham sido anonimizados pelo controlador (dados anonimizados ficam fora do escopo da LGPD);

- Informação sobre o compartilhamento

  O titular de dados pessoais tem o direito de saber quais são as entidades públicas e privadas com as quais a BlueShift realiza o compartilhamento dos seus Dados Pessoais;

- Informação sobre a possibilidade de não consentir

  O titular de dados pessoais tem o direito de receber informações esclarecedoras sobre a possibilidade e as consequências de não fornecer consentimento quanto ao tratamento de seus dados;

- Revogação do consentimento

O titular de dados pessoais pode retirar o seu consentimento. No entanto, todas as operações de tratamento de dados realizadas anteriormente a solicitação permanecem legais;

- Oposição

Na ausência de contrato ou consentimento direto junto a BlueShift, a ocorrência de tratamento de dados pode ocorrer, conforme previsto na LGPD. Nesse caso, somente haverá conforme justificativa prevista em lei, e o titular também poderá opor-se as finalidades destinadas ao tratamento em questão;

Em diálogo com nossos clientes, parceiros e fornecedores, promovemos direcionamento e acolhimento de questionamentos sobre as operações de tratamento de dados os quais estamos direta ou indiretamente envolvidos.

Enquanto operadores e gestores de sub-operadores, realizamos o registro das operações realizadas e conforme orientação dos controladores de dados, fornecendo as informações necessárias para promover respostas aos titulares de dados que solicitem esclarecimentos sobre as operações realizadas sobre seus dados.

Ademais, destacamos que são observadas também as limitações dos direitos dos titulares de dados os quais incluem-se os itens listados abaixo, nesses casos, a BlueShift poderá negar requisições do titular de dados:

- Proteção de propriedade intelectual da BlueShift, seus clientes, parceiros e fornecedores;
- Violação de direito de terceiros;
- Dados anonimizados;
- Obstrução de justiça;
- Interesses legítimos que sobrepõe os do titular de dados;
- Requisições excessivas ou reiteradas;
- Eliminação após o tratamento.

8. CANAIS DE COMUNICAÇÃO PARA TITULARES DE DADOS E ANPD

Com a finalidade de promover o diálogo e a melhoria contínua desta política, o titular poderá direcionar dúvidas, comentários ou sugestões através dos canais de contato abaixo:

DPO:

Esteban Huerta

E-mail: esteban.huerta@blueshift.com.br

Também disponibilizamos o canal para diálogo junto a Autoridade Nacional de Proteção de Dados

(ANPD) acessando o site https://www.gov.br/anpd/pt-br/canais_atendimento/

9. SEGURANÇA DA INFORMAÇÃO

Nos tópicos a seguir serão definidos normas, procedimentos e boas práticas de segurança da informação da BlueShift.

9.1. Regras de segurança da informação

As informações são acessadas apenas por pessoas devidamente autorizadas, como também todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas por essas pessoas, são de propriedade e uso exclusivo da BlueShift ou em casos contratuais de serviços ofertados pela BlueShift à clientes, tais informações são de propriedade do cliente;

Os colaboradores e parceiros devem zelar para que as informações tratadas, inseridas ou quando enviadas ao cliente ou em sistemas e procedimentos internos ou remotos da BlueShift, sejam livres de erro, transparentes e verídicas;

O acesso e uso das informações e recursos computacionais da BlueShift, por exemplo e-mail, devem estar limitados à ornada de trabalho ou período contratual do colaborador, exceto quando exercer atividade justificada ou plantões específicos devidamente controlados;

Todo e qualquer documento correspondente, bem como produzidos pela e/ou para BlueShift, não poderão sair fisicamente ou por meio digital das dependências ou locais de armazenamento da BlueShift sem explícita autorização prévia por pessoa que ocupe cargo ou função superior e assuma a responsabilidade por tal ação;

Quando necessária troca de informações com os clientes para cumprimento legal ou execução de tarefas inerente ao serviço contratado, é necessário utilizar os canais oficiais disponibilizados pela empresa. Qualquer outro tipo de canal ou meio utilizado, será considerado um descumprimento das regras de segurança da informação e serão tomadas as medidas cabíveis quanto ao fato;

9.2. Concessão, revogação e revisão

A concessão de acesso aos recursos tecnológicos da BlueShift deve estar atrelada aos perfis de acesso previamente atribuídos ao colaborador em razão da sua atividade profissional exercida.

A solicitação de acesso deve ser realizada pelo gestor do colaborador ao responsável de tecnologia via sistema de chamados com todas as informações do usuário cadastrado.

O responsável de tecnologia se reserva ao direito de revalidar as permissões, ou não, caso a concessão tenha mais permissões do que o definido em política interna para a efetiva concessão.

Todos os acessos concedidos serão revisados, no mínimo, a cada 6 (seis) meses, a fim de garantir que continuam ativos e atualizados.

A revogação de acesso deve ocorrer mediante solicitação do gestor responsável pelo colaborador ou parceiro ao responsável de tecnologia. No entanto, os direitos de acesso podem ser alterados e/ou revogados a qualquer tempo pela BlueShift, sem a necessidade de aviso prévio.

O acesso aos recursos tecnológicos será´ revogado imediatamente em caso de encerramento das atividades entre a BlueShift e as partes envolvidas. Portanto, assim que algum colaborador for demitido ou solicitar demissão, um parceiro tiver o contrato encerrado ou expirado, o responsável de TI tomará as providências necessárias.

9.3 Uso dos recursos de tecnologia da informação e comunicação

O colaborador deve utilizar apenas softwares e hardwares previamente homologados ou autorizados pelo responsável de tecnologia da BlueShift.

A gestão (instalação, manutenção e configuração) de todos os recursos tecnológicos é de responsabilidade exclusiva do responsável de tecnologia da BlueShift.

Todo colaborador ou parceiro que se distanciar de sua estação de trabalho ou do dispositivo móvel, deve imediatamente realizar o processo de bloqueio do equipamento.

Os equipamentos disponibilizados aos colaboradores e parceiros são de propriedade da BlueShift, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da organização, bem como cumprir as recomendações e normas mencionadas neste documento.

10. ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da BLUESHIFT, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada usuário de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Nosso compromisso com o tratamento das informações da organização, clientes e público em geral está baseado nos seguintes princípios:

10.1. Confidencialidade

As informações são acessadas apenas por pessoas devidamente autorizadas, para realizar a liberação de algum acesso o mesmo deve ser solicitado ao Gerente de Segurança da Informação da organização. Nesse caso, é dever do usuário impedir o acesso de quem quer que seja a tais informações, redobrando o cuidado com documentos e até mesmo com materiais deixados sobre as mesas ou em gavetas e armários.

10.2. Disponibilidade

As informações e os ativos correspondentes, estão disponíveis para acesso os usuários autorizados sempre que necessário.

10.3. Integridade

As informações armazenadas possuem suas características originais, não sofrendo alterações irrestritas em seu ciclo de vida.

11. RESPONSABILIDADES ESPECÍFICAS

11.1. Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da empresa.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a BLUESHIFT e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui estabelecidas.

11.2. Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

11.3. Gestores de Pessoas e/ou Processos

São responsabilidades dos gestores de Pessoas e/ou Processos:

- Servir de modelo de conduta para os colaboradores sob a sua gestão em relação à segurança da informação.
- Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência (Anexo I), assim como a responsabilidade do cumprimento da Política de Segurança da Informação da BLUESHIFT em todos os seus termos estabelecidos.

11.4. Área de Tecnologia da Informação

São responsabilidades da área de tecnologia da informação:

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política.
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a BlueShift.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
    - os usuários (logins únicos) individuais de funcionários serão de responsabilidade do próprio funcionário.
    - os usuários (logins únicos) de terceiros serão de responsabilidade do gestor da área contratante
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
    - uso da capacidade instalada da rede e dos equipamentos;
    - tempo de resposta no acesso à internet e aos sistemas críticos da BlueShift;
    - períodos de indisponibilidade no acesso à internet e aos sistemas críticos da BlueShift;
    - Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
    - Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

11.5. Área de Segurança da Informação

São responsabilidades da Área de Segurança da Informação:

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da BlueShift.
- Publicar e promover as versões da Política de Segurança da Informação e as Normas de Segurança da Informação aprovadas pela diretoria.
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da BlueShift, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

12. REGRAS

A Segurança da Informação na BLUESHIFT é regida pelas seguintes regras e diretrizes:

- As informações da organização e dos clientes devem ser tratadas de forma sigilosa, evitando a exposição indevida e mau uso.
- As informações devem ser utilizadas apenas para o fim específico de sua coleta.
- Informações devem ser compartilhadas respeitando níveis de acesso.
- As senhas das contas de serviço devem ser compartilhadas apenas entre os colaboradores da organização, respeitando os níveis de acesso.
- Todos os colaboradores podem contribuir para identificação e tratamento de vulnerabilidades.
- Informações da organização e de seus clientes devem ser transmitidas utilizando o e-mail corporativo.
- Agir de forma proativa para gerenciamento e segurança das informações.

13. POLÍTICA DE SENHAS

A política de senhas da BLUESHIFT é regida pelas seguintes diretrizes:

A. As senhas devem ser alteradas a cada três meses.
B. AS SENHAS devem cumprir os seguintes requisitos:
   - Mínimo de OITO caracteres
   - Conter letras MAIÚSCULAS
   - Conter NÚMEROS
   - Conter caracteres especiais (@!ˆ&)
   - Conter letras MINÚSCULAS

Em caso de desligamento de algum colaborador, todos os acessos dele devem ser revogados, e todas as senhas do ambiente devem ser alteradas. Tal ação visa garantir a integridade do ambiente.

Recomendamos que as senhas tenham sempre no mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial.

Recomendamos que as senhas também sejam ser trocadas pelos usuários a cada 3 meses, não devendo se repetir as senhas definidas nos últimos 12 meses.

Sempre que um usuário é desligado da organização, todas as suas senhas e acessos são revogados no mesmo dia.

• INDEPENDÊNCIA DAS DISPOSIÇÕES E DATA DA VERSÃO

As disposições desta política poderão ser objeto de alteração, com a finalidade de melhoria. Em hipótese de alteração por consideração de disposições invalidas, todas as demais permanecerão vigentes e inalteradas. A presente **Política de Segurança da Informação e Proteção de Dados** é publicada em **22/08/2022** em sua **versão 2.0.**