

Bell

Brazil



LGPD

Política de Segurança da Informação

SUMÁRIO

1. Contextualização	03
2. Definições	03
3. Escopo	06
4. Destinatários	06
5. Aplicabilidade	07
6. Objetivos	07
7. Princípios	08
8. Diretrizes	09
9. Deveres e Responsabilidades	11
10. Consequências em Caso de Violação	13
11. Atitudes de Comportamento Seguro	13



Tipo de documento:
POLÍTICA EMPRESARIAL

Código do documento:
POL.PSI - 0001

Número de
páginas: 16

Classificação da publicidade:
RESTRITO INTERNO

Nome de documento:
POLÍTICA DE SEGURANÇA
DA INFORMAÇÃO

Data de vigência:
13/06/2022

Versão:
V01/2022

1. Contextualização

A BELL AMFE possui o compromisso de estar adequado a LGPD, bem como garantir a proteção de dados, sejam pessoais ou não, que estão sob sua responsabilidade.

Assim, a presente Política de Segurança da Informação BELL AMFE (PSI BELL AMFE) apresenta as diretrizes orientativas e de conduta, além de determinar as responsabilidades que BELL AMFE possui com a intenção de mitigar eventuais riscos e danos relacionadas a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação.

2. Definições

AMEAÇA: evento que tem potencial em si próprio para comprometer os objetivos da empresa, seja trazendo danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas.

ATIVOS DE INFORMAÇÃO: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e compartilhadas pela BELL AMFE.

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

CLASSIFICAÇÃO DA INFORMAÇÃO: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear acesso.

CRİPTOGRAFIA: método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

DADOS PESSOAIS: Informação relacionada a pessoa natural identificada ou identificável. Também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural.

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

FORNECEDORES: No contexto da BELL AMFE são considerados fornecedores os outros terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais.

INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independente do suporte em que resida ou da forma pela qual seja vinculado.

INFRAESTRUTURA DE TECNOLOGIA DE INFORMAÇÃO: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, rede e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

LEI GERAL DE PROTEÇÃO DE DADOS (“LGPD”): Diploma normativo (Lei nº 13.709, de 14 de agosto de 2018) que dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo como objetivo defender os titulares de dados pessoais e ao mesmo tempo permitir o uso dos dados para finalidades diversas, equilibrando interesses e harmonizando a proteção da pessoa humana com o desenvolvimento tecnológico e econômico.

PARCEIROS COMERCIAIS: No contexto da BELL AMFE são considerados parceiros comerciais os terceiros contratados, sejam eles pessoa física ou jurídica, que atuam em seu nome: Consultores, Conveniados e Agentes Comerciais (aqueles que indicam atividades em que a BELL AMFE pode atuar como contratada).

QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

SEGURANÇA DE COMUNICAÇÕES: processo de proteção de dados digitais em trânsito.

SISTEMA ESTRUTURANTE: conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.

TERCEIRO: É toda pessoa física ou jurídica contratada pela BELL AMFE para desenvolver ou auxiliar no desenvolvimento de suas atividades, tanto na qualidade de fornecedores de bens ou serviços, como de parceiros comerciais.

TRATAMENTO DE DADOS PESSOAIS (“TRATAMENTO”): Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

VULNERABILIDADE: fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.

3. Escopo

A presente Política estabelece as diretrizes da BELL AMFE para proteção e uso de dados pessoais que venham a ser tratados em suas atividades, tendo como referência a Lei Geral de Proteção de Dados Pessoais, bem como os demais dados operacionalizados na empresa.

4. Destinatários

Esta Política se aplica a todos que se relacionam da BELL AMFE, seja Diretoria, empregados, estagiários, visitantes, parceiros comerciais que atuam em nome da BELL AMFE e fornecedores e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade da BELL AMFE.

A adesão à presente política é obrigatória a todos os destinatários acima indicados na medida em que se relacionam à BELL AMFE. O não cumprimento das disposições aqui previstas sujeitará o infrator às sanções previstas nesta política, sem prejuízo das medidas previstas em lei, caso se aplique

5. Aplicabilidade

Esta política estabelece diretrizes, regras, deveres e responsabilidades para garantir que todos os seus destinatários cumpram as leis de proteção de dados pessoais, bem como os padrões e medidas de segurança da informação da BELL AMFE.

6. Objetivos

São objetivos da Política de Segurança da Informação BELL AMFE:

- Estabelecer as diretrizes que assegurem e reforcem o compromisso da empresa com as práticas e medidas preventivas garantidoras de segurança da informação.
- Definir o referencial para a normatização das questões de segurança da informação.
- Criar condições para que a BELL AMFE eleve continuamente a sua maturidade em segurança da informação por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os ativos de informação da BELL AMFE visando a promoção da Integridade, Confidencialidade, Autenticidade e Disponibilidade dos ativos de informação da BELL AMFE.

- Descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela BELL AMFE que garantam a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

A presente Política deve ser lida em conjunto com as obrigações previstas nos documentos abaixo relacionados, que versam sobre informações em geral, e a complementam quando aplicável:

- I. Regimento Interno;
- II. Contrato de Trabalho;
- III. Código de Conduta; e
- IV Política de Privacidade e Proteção de Dados Pessoais.

7. Princípios

A BELL AMFE cumprirá com os seguintes princípios para que seja dado o devido tratamento ao ativo de informações:

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

8. Diretrizes

- A gestão da Segurança da Informação na BELL AMFE é de responsabilidade do setor de TI e do DPO.
- O cumprimento desta política deve ser avaliado periodicamente por meio de verificações periódicas, que deve ser realizada em um trabalho conjunto do setor de TI e do Comitê de Privacidade.
- A BELL AMFE, além desta política, se orienta pelas melhores práticas e procedimentos de segurança da informação recomendados pelo mercado.
- Os ativos de informação devem:
 - I. Ser inventariado e protegidos;
 - II. Ter identificados os seus proprietários e custodiantes;
 - III. Ter analisado as suas vulnerabilidades;
 - IV. Ter a sua entrada e saída nas dependências da BELL AMFE autorizadas e registradas pelo setor responsável;
 - V. Ser passível de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos; e

- VI. Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.
- A BELL AMFE possui critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade, sensibilidade, observando as legislações em vigor.
 - Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acesso indevido, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.
 - Todos os destinatários devem ter ciência:
 - I. Das ameaças e preocupações relativas à segurança da informação e;
 - II. De suas responsabilidades e obrigações no âmbito desta PSI.
 - Todos os destinatários devem difundir e exigir o cumprimento desta política.
 - Devem ser estabelecidos processos de revisão, de conscientização, de capacitação e de sensibilização em segurança de informação, que alcance a todos, conforme sua interação e responsabilidade dentro da BELL AMFE.
 - A BELL AMFE disponibiliza controle de acesso, de acordo com a relação do destinatário, das suas atividades e de suas responsabilidades, não podendo realizar o compartilhamento de senhas, logins e perfis.
 - Deve ser garantido a exatidão dos registros nos ativos de informação e relatórios, o que deve ser verificado em auditoria.

- Os usuários da BELL AMFE são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificação e assinatura digital.
- A identificação do usuário deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
- O acesso aos recursos computacionais e aos sistemas de informação deve ser limitado ao que é necessário, considerando a atribuição de cada usuário, e qualquer outra forma de acesso ou uso além do necessário depende de prévia autorização do gestor direto.

9. Deveres e responsabilidades

DEPARTAMENTO DE TI DEVE:

- a. aplicar e rever os controles de Segurança da Informação, como controle de acessos, senha/login, acesso ao servidor e outros;
- b. Dirimir eventuais dúvidas sobre a estrutura de informação;
- c. Analisar ataques e intrusões na rede da BELL AMFE;
- d. Executar as ações necessárias para tratar quebras de segurança;
- e. Obter informações mínimas acerca dos incidentes ocorridos, descrevendo sua natureza, causa, data de ocorrência, frequência e custos resultantes;

DPO E DEPARTAMENTO PESSOAL

- a. Apurar as ações que violem a PSI, devendo aplicar, aos que responsáveis, as sanções penais, administrativas e civis em vigor;

- b. Auxiliar e cooperar com o Departamento de TI no incidentes de segurança;
- c. Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- d. Informar aos ingressos sobre a Política e Procedimentos de Segurança da Informação adotados pela BELL AMFE;
- e. Elaborar e aplicar, sob a orientação da Gerência de Tecnologia da Informação, treinamento sobre Segurança da Informação na BELL AMFE, sempre que necessário;
- f. Informar, prontamente, à área de TI, todos os desligamentos, afastamentos e modificações no quadro funcional da empresa;
- g. Orientar e indicar as consequências que entenderem cabíveis para os que violarem esta política, cabendo à Diretoria definir se concordam ou não com a decisão indicada.

SETOR GERENCIAL

- a. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- b. Assegurar que suas equipes possuam acesso e conhecimento da Política, das Normas e dos Procedimentos de Segurança da Informação;
- c. Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados;
- d. Formalizar toda a inserção, alteração ou exclusão de acesso ao sistema para a setor de TI e para o DPO, em especial o sistema de monitoramento de segurança eletrônica; e
- e. Comunicar imediatamente eventuais casos de violação de segurança da informação ao DPO.

10. Consequências em caso de violação

O descumprimento desta política por parte de um integrante, este se sujeitará, além das penalidades legais, às medidas trabalhistas disciplinares, o que inclui, em última instância, a rescisão do contrato de trabalho por justa causa ou rescisão antecipada do contrato existente, além das medidas penais cabíveis.

No caso do descumprimento por parte de Terceiros, Parceiros, Fornecedores ou Clientes, estes se sujeitarão, além das penalidades legais e ações civis cabíveis, à aplicação de multa e rescisão motivada ou antecipado contrato.

11. Atitudes de comportamento seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da BELL AMFE, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários, estagiários e prestadores de serviços devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações da BELL AMFE.
- Os colaboradores da BELL AMFE devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Todo tipo de acesso à informação da BELL AMFE que não for explicitamente autorizado é proibido.
- Informações confidenciais da BELL AMFE não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido.
- Somente softwares homologados pela BELL AMFE podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe da Gerência de Tecnologia da Informação.
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados.

- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação da Gerência de Tecnologia da Informação da BELL AMFE.

Elaboração:
TI

Data: 10/06/2022

Revisão:
DPO

Data: 10/06/2022

Aprovação:
ALTA ADMINISTRAÇÃO

Data: 13/06/2022

Bell

Brazil

CANAL DE DENÚNCIA E INTEGRIDADE:

(62) 3121-4721

www.aintegridade.com.br/bell



Aintegridade

(62) 4016-2001

Av. Deputado Jamel Cecílio, 2.690, Ed. Metropolitan Business,
Torre Tokyo, Sala 903 - Jardim Goiás, Goiânia/GO

fbrcompliance.com.br

aintegridade.com.br