Sumário

As organizações enfrentam diversas ameaças que podem comprometer informações e ativos, afetando a confidencialidade, integridade e disponibilidade dos dados. Isso pode resultar em perdas operacionais, financeiras, de reputação, multas e quebras contratuais.

Proteger a informação é crucial para manter a competitividade, fluxo de caixa, lucratividade, conformidade legal e imagem da organização. A segurança da informação da **Be Aliant** é mantida através de controles adequados, incluindo políticas, processos, procedimentos e tecnologias.

Além disso, a segurança da informação visa proteger ativos informacionais e reduzir riscos como acessos não autorizados, uso indevido, fraudes, roubo, sabotagem e negação de serviço. Os principais objetivos são:

- Confidencialidade: Garantir que apenas pessoas autorizadas tenham acesso às informações.
- Integridade: Assegurar que as informações permaneçam inalteradas sem modificações indevidas.
- Disponibilidade: Assegurar que as informações estejam acessíveis para pessoas autorizadas.

1. APLICABILIDADE

A Política de segurança da informação da Site - **Be Aliant**, aplica-se a todas as partes interessadas, como prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, caso utilizem o ambiente de processamento, ou acesso a informações pertencentes à **Be Aliant**. Todo e qualquer usuário tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos. A violação desta política de segurança é qualquer ato que:

a) Exponha a Companhia a uma perda efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento.
b) Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
c) Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

2. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da **Be Aliant**.

3. MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da **Be Aliant**. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

4. DEVERES

a) É dever da **Be Aliant** considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor e necessita sempre ser tratada profissionalmente.

b) A responsabilidade pela criação e manutenção deste documento é da área de Tecnologia da Informação.

c) Todas as partes interessadas devem cumprir as diretrizes desta política, sendo que o descumprimento acarretará a aplicação das medidas administrativas e legais cabíveis.

d) Todo incidente ou fato duvidoso que afete a segurança da informação, deverá ser comunicado inicialmente à área de Tecnologia da Informação da **Be Aliant** através do endereço helpbe@becompliance.com.

e) A **Be Aliant** se reserva ao direito de solicitar o preenchimento de relatório de verificação de Cyber Segurança de fornecedores.

5. DO MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas na política de segurança da informação, a **Be Aliant** poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, não se limitando aos aqui descritos.

b) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

c) Aplicar controles apropriados, trilhas de auditoria ou registros de atividades para mitigar riscos.

6. USO DE INFORMAÇÕES

Com relação às informações os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou acesso a informações pertencentes à **Be Aliant** venham a tomar conhecimento:

a) É proibida a divulgação e/ou o compartilhamento indevido de informações sem a devida autorização.

b) Apenas os autorizados pela **Be Aliant** podem copiar, captar, imprimir ou enviar imagens da tela do software para terceiros.

c) As partes interessadas assumem o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na **Be Aliant**, mesmo depois de terminado o vínculo contratual mantido com a instituição.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

A Be Aliant estabeleceu critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada de acordo com a tabela abaixo:

Informação Pública	É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna	É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
Informação Restrita	É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
Informação Confidencial	É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

8. DADOS DE TERCEIROS

A **Be Aliant** se compromete em não acumular ou manter intencionalmente Dados Pessoais de Terceiros além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais que porventura sejam armazenados, serão considerados dados confidenciais.

Dados Pessoais sob a responsabilidade da **Be Aliant** não serão usados para fins diferentes daqueles para os quais foram coletados, e nem serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da **Be Aliant**.

9. PROGRAMAS ILEGAIS

A empresa respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. Dessa forma, repudiamos a utilização de programas ilegais (Sem licenciamento).

Todos os usuários não podem, em hipótese alguma, instalar este tipo de “software” (programa) nos equipamentos da **Be Aliant**, mesmo porque somente o pessoal da área de TI tem autorização para instalação de programas previamente autorizados dentro da política de segurança da companhia.

Periodicamente, o Setor de TI faz verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

A **Be Aliant** se isenta de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

10. PERMISSÕES E SENHAS

Todos os terceiros que necessitarem acessar a rede da Be Aliant devem ter credenciais cadastradas pelo Departamento de TI. Eles são responsáveis pelo uso adequado de suas credenciais, em conformidade com a legislação.

O compartilhamento de logins e senhas é proibido, e as senhas devem ser atualizadas periodicamente. Além disso, em caso de término do vínculo, o setor responsável deve informar ao Departamento de TI para desabilitar o acesso.

11. COMPARTILHAMENTO DE DADOS

A Be Aliant adota rigorosos controles de segurança em relação ao compartilhamento de dados, visando garantir a confidencialidade e integridade das informações.

Não é permitido o compartilhamento de pastas em dispositivos de computadores ou desktops dentro da empresa. Todos os dados devem ser armazenados exclusivamente na nuvem, com acesso autorizado pelo Departamento de TI, que gerencia e monitora as permissões de forma centralizada.

O Departamento de TI realiza auditorias periódicas nos dispositivos para garantir que dados confidenciais e/ou restritos não estejam armazenados localmente, garantindo a conformidade com as políticas de segurança.

Além disso, o compartilhamento de impressoras está sujeito à autorização prévia do Departamento de TI. Dispositivos móveis, como pen-drives e outros, não são permitidos para transferência de dados, reforçando a segurança no ambiente corporativo.

12. SEGURANÇA E INTEGRIDADE DOS DADOS

Na **Be Aliant** gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Departamento de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

13. PENTEST

Com objetivo de identificar vulnerabilidades de segurança em sistemas, softwares e redes, a fim de melhorar as medidas de segurança e proteção dos ativos da empresa contra ataques cibernéticos, a equipe de TI:

a. Deve realizar, **de forma anual, testes de intrusão, podendo alternar entre a execução de um Pentest completo em um ano e o respectivo reteste no ano subsequente**;
b. É responsável por coordenar e aprovar todos os testes de intrusão;
c. Deve fornecer acesso aos sistemas autorizados para a realização dos testes de intrusão;
d. Necessita que os testes de intrusão sejam realizados de acordo com as melhores práticas e diretrizes de segurança;

e. Precisa conduzir o teste de forma a minimizar qualquer impacto nos sistemas e serviços em produção;
f. Deve tratar todas as informações obtidas durante os testes de intrusão como confidenciais, protegendo-as contra acesso não autorizado.

14. PROPRIEDADE INTELECTUAL

A prática do uso de software pirata ou conteúdo não legalizado é um crime previsto na Lei 9.609/1998, e vai contra diretrizes de compliance com relação à segurança da informação e privacidade.

Assim, a instalação de softwares ou aplicações piratas constitui crime contra a propriedade intelectual, sujeitando os infratores às penalidades previstas na legislação. Somente devem ser instalados softwares com contratos de licenciamento vigentes e homologados pelo Departamento de Tecnologia da Informação.

Desta forma, a **Be Aliant** proíbe a utilização de qualquer tipo de software ou conteúdo não legalizado. Devendo ainda cada funcionário estar ciente de que todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício, são de propriedade da **Be Aliant**.

15. USO DA INTERNET

A internet corporativa da **Be Aliant** deve ser utilizada exclusivamente para fins profissionais, enriquecimento intelectual e busca de informações que contribuam para o desenvolvimento das atividades da empresa.

O uso da internet para assuntos pessoais, como home banking e lojas virtuais, é permitido com moderação, desde que seja feito com bom senso e em conformidade com as diretrizes corporativas.

É estritamente proibido acessar sites impróprios, incluindo, mas não se limitando a jogos, mensagens de corrente, troca ou armazenamento de conteúdo ilícito, obsceno, pornográfico, violento, discriminatório, racista, político, religioso, difamatório ou desrespeitoso, conforme as Leis nº 8.069 (Estatuto da Criança e do Adolescente) e nº 12.965 (Marco Civil da Internet).

Os acessos à internet corporativa são monitorados por meio da identificação do usuário e podem ser bloqueados a qualquer momento, sem aviso prévio, pela equipe de tecnologia ou segurança da informação, caso seja identificada alguma irregularidade ou risco ao ambiente.

Essa política visa garantir um uso responsável e seguro da internet no ambiente corporativo, alinhado aos valores e objetivos da Be Aliant.

16. ACESSO REMOTO E VPN

Na **Be Aliant**, o acesso remoto a recursos de tecnologia e informações corporativas, quando realizado fora das instalações da empresa, deve ser feito exclusivamente por meio da tecnologia Virtual Private Network (VPN).

A concessão de acesso remoto via VPN aos colaboradores requer autorização formal da Direção da Be Aliant, de acordo com as necessidades profissionais de cada colaborador.

O Departamento de Tecnologia da Informação (TI) é responsável por gerar relatórios contendo todos os acessos realizados via VPN. Esses relatórios ficam disponíveis para consulta pela Direção, caso seja necessário.

17. USO DO CORREIO ELETRÔNICO (EMAIL) E INSTANT MESSENGER

O correio eletrônico (e-mail) fornecido pela Be Aliant é uma ferramenta de comunicação corporativa exclusiva para a realização das atividades profissionais da empresa. Apenas programas e plataformas homologados pelo Departamento de Tecnologia da Informação (TI) podem ser utilizados para enviar e-mails.

As mensagens enviadas por e-mail devem ser redigidas em linguagem profissional, respeitando os princípios éticos da Be Aliant e a legislação vigente. O uso do e-mail é pessoal e cada colaborador é responsável pelo conteúdo das mensagens enviadas de seu endereço de e-mail corporativo.

18. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O Departamento de Tecnologia da Informação (TI) da Be Aliant é responsável pela implementação e aplicação das políticas internas relacionadas à aquisição e substituição de software e hardware.

Qualquer necessidade de novos programas (softwares) ou equipamentos de TI (hardwares) deve ser discutida diretamente com o responsável pelo Departamento de TI. Não é permitido que os usuários comprem ou desenvolvam software ou hardware de forma independente.

19. USO DO NOTEBOOK NA BE ALIANT

Dispositivos corporativos e recursos tecnológicos são disponibilizados exclusivamente para atividades profissionais, com o objetivo de assegurar a segurança e a integridade das operações da Be Aliant.

Os equipamentos fornecidos são de propriedade da empresa e não devem ser utilizados para fins pessoais, atividades ilícitas ou acesso a conteúdos que violem a legislação vigente. Alterações ou manutenções nos dispositivos são realizadas apenas pelo departamento de Tecnologia da Informação (TI).

Todos os dispositivos devem contar com software antivírus atualizado e ativo. Em caso de problemas técnicos, o departamento de TI deve ser acionado imediatamente. A Be Aliant reserva-se o direito de inspecionar os dispositivos corporativos a qualquer momento, garantindo seu uso correto e adequado.

20. RESPONSABILIDADE DOS GERENTES/SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da **Be Aliant**, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Departamento de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

a) Que tipo de informação o usuário pode acessar;
b) Quem está autorizado a acessar determinada rotina e/ou informação.

21. SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da **Be Aliant**, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Departamento de TI, de acordo com as definições da Diretoria da **Be Aliant**.

22. COMUNICAÇÃO INTERNA E EXTERNA

A comunicação interna e externa desempenha um papel crucial na efetividade do sistema de gestão da segurança da informação na **Be Aliant**. Desta forma, métodos e práticas devem ser dotados para garantir uma comunicação interna eficiente, que conceda transparência dentro e fora da **Be Aliant**.

22.1. Comunicação Interna:

Com relação a comunicação interna, consideramos essencial manter todos os colaboradores informados sobre assuntos de grande importância e relevância, tais como procedimentos, políticas, treinamentos, entre outros. Recomendamos para comunicação os seguintes meios:

Newsletters via e-mail: Enviamos newsletters regularmente aos colaboradores, abordando sobre eventos internos e outras informações relevantes. Acreditamos que esse meio, mantém todos os membros da empresa atualizados e engajados.

Módulo de "NEWS" nas plataformas da Be: Nossas plataformas internas possuem um módulo dedicado às notícias e conteúdos. Por meio dessa funcionalidade, compartilhamos informações em tempo real, o que facilita o acesso e a disseminação de conhecimentos importantes para todos os colaboradores.

Documentos Internos: Utilizamos o módulo "Documentos" em nossas plataformas para divulgar documentos internos, como políticas de segurança, procedimentos operacionais, comunicações e outras diretrizes. Além disso, esse sistema também permite coletar assinaturas eletrônicas para garantir a conformidade dos colaboradores com as políticas estabelecidas.

22.2. Comunicação Externa:

A comunicação externa é igualmente relevante, especialmente quando se trata de compartilhar informações com partes interessadas externas à Be Aliant. Nesse sentido, seguimos as diretrizes do requisito 7.1 da ISO 27001/2022:

a) O que comunicar: Sempre analisamos o que iremos comunicar para cada vez mais reforçar a confiança e nosso compromisso com a excelência e responsabilidade com as partes externas. Quando comunicado utilizamos nossas newsletter para comunicação sobre atualizações da plataforma, novidades, aspectos que impactem na segurança da informação, e outros relevantes.

b) Quando comunicar: Priorizamos a comunicação oportuna, garantindo que informações sejam compartilhadas rapidamente.

c) Com quem comunicar: Identificamos as partes interessadas externas relevantes e garantimos que a comunicação seja direcionada especificamente a elas, nos ajudando que a mensagem seja direcionada para partes relevantes.

d) Como se comunicar: Utilizamos meios confiáveis de comunicação externa, como e-mails, canal de suporte com o cliente, newsletters, e outros métodos apropriados para garantir a confidencialidade, integridade e disponibilidade das informações compartilhadas.

23. BACKUP

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da **Be Aliant**, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Departamento de TI, de acordo com as definições da Diretoria da **Be Aliant**.

A gestão de Backup deve seguir as melhores práticas da norma técnica da ABNT ISO/IEC 27002.

Todos os backups de sistemas, servidores e serviços de TI devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup”, que são períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

a) Todos os restores (recuperação de dados que estão em backup) deverão ser formalizados, sem exceção, através do sistema de aberturas de solicitação ao departamento de Tecnologia da Informação.
b) É proibido a realização de backups em dispositivos de mídia removíveis - HDs Externos, Pendrives ou dispositivos similares – ou em serviços de armazenamento em nuvem não corporativo.

24. MESA E TELA LIMPA

Conforme política própria, todos da empresa devem adotar o princípio de mesa limpa e tela limpa, para redução de riscos de acesso não autorizado, perda ou danos às informações. Para isso, as seguintes recomendações devem ser observadas:

a) Papéis e mídias eletrônicas, quando não em uso, devem ser armazenados em armários trancados ou mobiliários seguros.
b) Nenhuma anotação deve ser deixada à mostra sobre a mesa, computador ou divisórias, mesmo com o colaborador presente.
c) Informações confidenciais devem ser mantidas trancadas em local separado quando não em utilização.
d) Informações confidenciais não devem ser anotadas em quadros brancos e/ou salas de reunião.
e) Documentos devem ser destruídos (picotados) antes do descarte.
f) Ao imprimir, retire imediatamente seu documento da impressora.
g) Computadores não devem ser deixados autenticados quando não houver um colaborador junto, e devem ser protegidos por senha.
h) Em todos os computadores, deve ser configurado um protetor de tela, que solicite senha ao ser solicitado acesso ao computador.

25. USO DO ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa a **Be Aliant** deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado.

A atualização do antivírus será automática, agendada pelo próprio sistema, e auditada pelo Departamento de TI. O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

26. APLICAÇÕES EM NUVEM

As responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem para serviços em nuvem devem ser claramente definidas e acordadas.
Terceiros devem aderir aos requisitos estabelecidos nesta Política de Gerenciamento de Vulnerabilidades (PGV). Sempre que possível, as obrigações relacionadas ao gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

Recomenda-se que a Be Aliant, ao utilizar serviços em nuvem, verifique se o provedor assegura a gestão técnica de vulnerabilidades dos recursos oferecidos.

Além disso, deve ser observado se as responsabilidades do provedor de serviços em nuvem para a gestão de vulnerabilidades estão dispostas no contrato de serviços, e que inclua os processos para relatar as ações do provedor.

27. DO ARMAZENAMENTO DE DADOS

A **Be Aliant** se compromete em não acumular ou manter intencionalmente Dados Pessoais além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais que porventura sejam armazenados, serão considerados dados confidenciais.

Os seus dados pessoais poderão ser compartilhados com nossos parceiros de negócios e prestadores de serviços terceirizados, de acordo com a legislação, os quais não estão autorizados a compartilhar ou utilizar tais informações para qualquer finalidade que não seja a prestação de seus serviços; e terceiros que necessitem processar seus Dados Pessoais para proteção de nossos direitos.

Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores **Be Aliant**, e jamais poderão fazer parte da rotina de backup da empresa.

28. CONSCIENTIZAÇÃO E TREINAMENTO

A **Be Aliant** se compromete a conscientizar colaboradores e, quando aplicável, demais partes interessadas por meio de treinamentos e campanhas sobre segurança da informação, realizados periodicamente, pelo menos uma vez ao ano.

29. USO DO E-MAIL

O e-mail corporativo da Be Aliant deve ser utilizado exclusivamente para fins profissionais e atividades relacionadas às operações da empresa. Recomenda-se que todas as comunicações oficiais com a Be Aliant sejam realizadas

através de e-mails corporativos, assegurando a confidencialidade e integridade das informações. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias, linguagem ofensiva ou conteúdos inadequados;
- Prejudiquem a imagem da Be Aliant ou de outras empresas;
- Divulguem informações não públicas sem autorização prévia;
- Estejam relacionadas a atividades ilícitas ou violem a legislação vigente.

A Be Aliant reserva-se o direito de monitorar e inspecionar informações transmitidas por seus e-mails corporativos, visando garantir a segurança e o alinhamento às suas políticas.

30. CONTROLE DE ACESSO

a) O acesso à VPN da Be Aliant deve ser usado exclusivamente para atividades profissionais e relacionadas aos negócios da empresa.
b) É essencial que os usuários desconectem a VPN quando não estiverem utilizando-a e mantenham a conexão ativa apenas pelo tempo necessário para concluir suas tarefas.
c) Além disso, todos os usuários devem ter uma identificação única e intransferível, sendo responsáveis por qualquer atividade realizada com suas credenciais.
d) As senhas devem ser fortes, compostas por pelo menos oito caracteres, incluindo números, letras maiúsculas e minúsculas e caracteres especiais.
e) É importante que as senhas não sejam baseadas em informações pessoais facilmente obtidas.
f) Os usuários devem memorizar suas senhas e evitar anotá-las.
g) Senhas não devem ser incluídas em processos automáticos de acesso ao sistema.

31. CONTINUIDADE DE NEGÓCIO

A **Be Aliant** deve manter planos e processos para assegurar a operação contínua da empresa, minimizando os impactos aos clientes, mesmo em situações de desastre, até o restabelecimento completo das atividades.

Esses planos devem estar sempre alinhados às necessidades do negócio e passar por revisões e testes periódicos.

A empresa conta com um Plano de Continuidade de Negócios e Procedimento de Gestão de Incidentes, que estabelecem diretrizes e controles claros sobre este tema.

32. PENALIDADES

O não cumprimento desta Política de Segurança da Informação é considerado uma falta grave e poderá resultar em ações corretivas por parte do Comitê de Ética da Be Aliant, e/ou medidas previstas na legislação vigente.

Caso haja suspeita de violação desta política, comunique imediatamente ao canal de denúncias da Be Aliant pelos seguinte meio:

Online: https://we.bealiant.com/canal-etica/canal-denuncias

Essas medidas aplicam-se a todos os colaboradores e partes interessadas.

33. REVISÃO

A revisão da política interna ocorrerá no mínimo de forma anual. Além disso, a revisão poderá ser realizada a qualquer momento em que a **Be Aliant** identificar a necessidade, seja devido a mudanças regulatórias, novas diretrizes internas ou outras circunstâncias que possam impactar a eficácia ou aplicação das políticas.

34. CONTROLE DO DOCUMENTO

Revisão	*Data Revisão*	*Histórico da Revisão*	*Elaborado por*	*Aprovado por*
00	12/12/2024	Emissão inicial.	Wellington Faria – Gestor SGSI – SGPI	Akihito Kumon - Direção
01	18/08/2025	Realizada revisão com relação ao tópico sobre PENTEST.	Wellington Faria – Gestor SGSI – SGPI	Akihito Kumon - Direção
02	06/04/2026	Realizada revisão para refletir nova realidade Be Aliant.	Wellington Faria – Gestor SGSI – SGPI	Fernando Scanavini - Direção