# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## SUMÁRIO:

## OBJETIVO:

Estabelecer as diretrizes, controles e princípios relacionados à segurança da informação (SI), visando a redução de riscos e a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI); Além de assegurar a confidencialidade, integridade e a disponibilidade da informação, a continuidade do negócio, e o conformidade à legislação vigente, normas e boas práticas de mercado.

## APLICAÇÃO E ABRANGÊNCIA:

Aplica-se a todos os usuários com acesso às informações da Produtos Alimentícios Orlândia S/A Comércio e Indústria - Brejeiro e empresas do grupo, independentemente do seu vínculo com a empresa, ou seja, gestor, colaborador, estagiário, temporário, terceiro, prestador de serviço ou de qualquer forma no âmbito de Representante e/ou Parceiro de Negócios.

## CONCEITOS/GLOSSÁRIO:

Utilizar o documento Conceitos Gerais / Glossário Único da Produtos Alimentícios Orlândia S/A Comércio e Indústria – Brejeiro.

## REFERÊNCIAS E SITAÇÕES:

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas da Produtos Alimentícios Orlândia S/A Comércio e Indústria – Brejeiro, para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A PSI segue as leis vigentes no Brasil e foi elaborada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, NIST Cybersecurity Framework 2.0, CIS Critical SecurityControls Version 8, reconhecidos mundialmente como um código de prática para a gestão da segurança da informação. Paralelamente, foi desenvolvida uma Política de Segurança da Informação Educacional para aumentar a segurança da infraestrutura tecnológica direcionada ao uso acadêmico.

Documentos citados nesta política:

- Política de Código de Ética e Conduta
- Política de Gestão e Governança de Dados
- Norma de Gestão de Ameaças e vulnerabilidades
- Norma de Gestão de Identidades e Acessos Lógicos
- Norma de Gestão e Configuração de Senhas
- Norma de Gestão de Acessos Físicos
- Norma de Classificação da Informação
- Norma de Gestão de desenvolvimento Seguro
- Norma de Gestão de Segurança em CLOUD – CLOUD Security
- Norma de Gestão de BYOD
- Norma de Gestão de DLP
- Norma de Gestão de Ativos
- Norma de Gestão de Riscos Tecnológico
- Norma de Gestão de Incidentes
- Norma de Gestão de Logs e Trilhas de Auditoria
- Norma de Gestão de Backup e Restore
- Norma de Gestão de Continuidade de Negócio
- Norma de Gestão de Riscos Corporativos
- Procedimento Conheça seu Parceiro (Gestão de terceiros e fornecedores)
- Procedimento de Conscientização de Segurança
- Procedimento de Gestão de Configurações de Segurança e Patches
- Procedimento de Respostas a Incidentes de SI
- Procedimento de Monitoramento e Logs e Eventos de SI
- Procedimento de Gestão de Suporte TI
- Procedimento de Respostas a Incidentes de TI
- Procedimento de Monitoramento e Logs e Eventos de TI
- Procedimento de Respostas a Incidentes de Negócio

# INTRODUÇÃO E CONTEXTO:

## • POR QUE A SEGURANÇA DA INFORMAÇÃO É NECESSÁRIA?

As organizações são expostas a diversos tipos de ameaças, que podem causar incidentes e comprometer as informações e seus ativos por meio da exploração de vulnerabilidades, materializando riscos que afetam a confidencialidade, integridade e a disponibilidade da informação. E, consequentemente, causando impactos negativos tangíveis ou intangíveis aos negócios, tais como, perda operacional, financeira ou de imagem, aplicação de multas, quebra contratual, entre outros.

"...definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado" (ABNT, NBR ISO/IEC 27002).

Neste contexto, definir, estabelecer, manter e aprimorar a segurança da informação são atividades essenciais para mitigar riscos que podem causar prejuízos à organização, buscando a continuidade de seus negócios.

"A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções tecnológicas de software e hardware" (ABNT, NBR ISO/IEC 27002)

## • OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da informação tem como objetivos a proteção dos ativos de informação, a redução dos riscos de acessos não autorizados, uso indevido da informação ou dos sistemas, redução dos riscos de fraude financeira ou roubo, risco de alteração de atividade comercial (por exemplo, sabotagem, negação de serviço), além da capacidade de identificar, proteger, detectar, responder e recuperar rapidamente uma ameaça cibernética, a fim de proteger os ativos tecnológicos e informações auxiliando a empresa a cumprir sua missão e valores.

Desta forma, os objetivos principais são:

- **CONFIDENCIALIDADE**: Garantir que as informações tratadas sejam de conhecimento 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 às pessoas autorizadas.

## DIRETRIZES GERAIS:

É diretriz que, toda informação de propriedade da Brejeiro, seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

Todo produto ou informação gerada, processada, transmitida, armazenada por qualquer colaborador constitui ativo de propriedade intelectual da Brejeiro e essencial à condução de seus negócios.

Independentemente da forma apresentada que pode ser de forma física, eletrônica, escrita ou falada, ou como ela é compartilhada, armazenada ou transmitida, a informação deve ser utilizada unicamente à finalidade à qual foi autorizada e não deve ser utilizada em meios não autorizados.

Todos os esforços de segurança da informação devem ser projetados, implantados e mantidos buscando proteger os requisitos de negócio da Brejeiro;

Os princípios gerais de segurança aqui descritos devem ser desdobrados em outras políticas, normas e procedimentos adequados à sua correta execução, além de controles e monitoramentos necessários;

A Brejeiro reserva-se o direito de, a qualquer momento e sem aviso prévio, monitorar, auditar, bloquear ou fazer cópias de Segurança de qualquer dado e/ou informações armazenados em ativos de sua propriedade ou que trafegam em sua rede, assim como de qualquer tipo de acesso físico ou lógico em seus sistemas e ambientes;

Situações específicas que não estejam contempladas ou sejam conflitantes com esta política, devem ser tratadas pelas áreas de Compliance e Segurança da Informação, sendo as decisões justificadas, documentadas e aprovadas pelas partes envolvidas;

## COMITE DE SEGURANÇA DA INFORMAÇÃO:

Deve ser estabelecido um comitê para definir, coordenar e tomar decisões pertinentes, assim como deliberar sobre os principais aspectos de segurança da informação, garantindo que os projetos e iniciativas sejam entendidos, avaliados e priorizados pela Alta Direção;

## MEMBROS DO COMITE SI:

Comitê de Segurança da Informação será composto pelos seguintes membros permanentes:

- Diretor Geral;
- Diretor de Inovação;
- Gerente TI;
- Gerente RH;
- Gerente de Controladoria;
- Assessor Jurídico;
- Analista de Infraestrutura;

Adicionalmente, conforme a pauta e convite, poderão agregar-se ao comitê outras pessoas;

Em caso de ausência, os membros permanentes devem designar seus representantes, com autonomia para tomada de decisões sobre assuntos que serão discutidos no comitê;

## ORGANIZAÇÃO DO COMITE DE SI:

O Gerente de TI juntamente com a Assessora Jurídica possui a função de Coordenador do Comitê de Segurança da Informação, sendo responsáveis por convocar as reuniões, coordenar e controlar a participação dos membros, assim como elaborar as pautas e gerir a documentação e os assuntos de interesse do Comitê;

O Comitê deve se reunir minimamente uma vez ao ano, e/ou de forma extraordinária quando convocado pelo Coordenador do Comitê para tratamento de assuntos específicos e/ou urgentes;

Os assuntos pautados devem ser deliberados com prioridade pelo Comitê, em detrimento a assuntos não inseridos em pauta previamente;

Qualquer membro permanente do Comitê possui alçada para sugerir um assunto para ser discutido na reunião, desde que previamente informado ao Coordenador do Comitê;

A aprovação de assuntos da pauta do Comitê, quando necessário, deve ser realizada por consenso dos membros. Para efeito de consenso será observado o conceito de maioria presente na reunião em questão;

## SEGURANÇA EM RECURSOS HUMANOS:

Deve ser estabelecido processos formais dentro da organização para que todos os colaboradores, terceiros e prestadores de serviço, tenham acesso e ciência das diretrizes e orientações descritas nesta política e suas derivadas.

Deve ser estabelecido termos de confidencialidade ou semelhantes para todos os colaboradores, terceiros e prestadores de serviço, que tenham acesso a informações de propriedade da Brejeiro, de forma a promover maior nível de comprometimento e responsabilidade.

Quando houver processos da organização, utilização de prestadores de serviços, fornecedores e/ou parceiros de negócio, deve ser estabelecido através de contratos com as empresas, cláusulas que contemplem a obrigatoriedade de aderência as diretrizes estabelecidas nesta política e derivadas.

## CONSCIENTIZAÇÃO E TREINAMENTOS:

Deve ser promovido treinamentos e conscientizações periódicas, com foco em Segurança de informação, para todos os seus colaboradores, terceiros e prestadores de serviço, mais detalhes devem ser observados no “**Procedimento de Conscientização de Segurança**”.

## USO DE CORREIO ELETRÔNICO:

O uso do correio eletrônico é voltado exclusivamente para fins corporativos e relacionados às atividades do colaborador dentro da instituição.

É vedado utilização de e-mails corporativo para cadastro em sites externos que não estejam relacionados aos processos da empresa e para fins corporativos (ex.: Blogs, fóruns, jogos, redes sociais, sites de compras etc.).

Toda comunicação de e-mails com parceiros, fornecedores, clientes ou prospects, devem ser obrigatoriamente realizados através de e-mails corporativos;

É vedado o acesso a e-mails pessoais utilizando webmails ou qualquer outra ferramenta, mesmo quando as políticas de proteção não bloquearem automaticamente o acesso.

A Brejeiro se reserva o direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas via e-mail corporativo.

## USO DE INTERNET:

A Internet corporativa deve ser utilizada exclusivamente para fins corporativos, enriquecimento intelectual ou como ferramenta de busca por informações, enfim, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O uso da internet para assuntos pessoais (home banking, lojas virtuais e afins) é permitido, com limitações, desde que com bom senso e respeitando as demais diretivas corporativa.

Não é permitido os acessos a sites impróprios na Internet, 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 que desrespeite qualquer indivíduo ou entidades, de acordo com as Leis nº 8.069 (Estatuto da Criança e do Adolescente) e nº 12.965 (Marco Civil da Internet).

Os acessos a internet corporativa são monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento, sem aviso prévio, pela equipe de tecnologia ou segurança da informação, quando for identificado alguma irregularidade ou risco ao ambiente.

## USO DE MIDIAS SOCIAIS:

Todos os assuntos relacionados a comunicação externa e mídias sociais devem ser centralizado nas áreas marketing, comunicação ou áreas formalmente autorizadas, desta forma nenhum colaborador, terceiro, prestador de serviços e/ou parceiros pode através de meios de comunicação, mídias sociais ou sites externos, publicar, comentar ou ter atitudes semelhantes, em nome da Brejeiro, sem autorização formal.

## USO DE SOFTWARES DE MENSAGERIA:

A Brejeiro autoriza o uso das ferramentas SPARK e WEBEX para a comunicação interna de seus colaboradores, sendo proibida a transferência ou compartilhamento de arquivos ou quaisquer informações confidenciais para fora da rede corporativa.

## USO DE COMPUTADORES CORPORATIVOS:

Os recursos corporativos devem ser utilizados com responsabilidade e exclusivamente para atividades relacionadas a empresa.

Os usuários devem ter zelo pelos recursos corporativos, como computadores, impressoras, celulares e demais equipamentos, podendo sofrer sanções administrativas.

Não é permitido que usuários sejam administradores de suas máquinas, exceções devem ser avaliadas, justificadas e documentadas através do fluxo de exceções;

Não é permitido instalar ou executar softwares não licenciados, ou considerados “piratas”, assim como softwares não homologados nos ativos corporativos.

A imagem do sistema operacional dos equipamentos corporativos deve ser padronizada e homologada pela equipe de SUPORTE_TI, devendo ser atualizada periodicamente e mantendo sempre as atualizações de segurança mais recentes.

A manutenção e configuração dos computadores corporativos é de responsabilidade exclusiva da equipe de SUPORTE_TI, sendo vedado aos demais colaboradores alterarem suas configurações, abrir o equipamento ou alterar componentes, sem autorização formal.

Todos os incidentes corporativos que envolvam as máquinas corporativas, incluindo, mas não se limitando a vulnerabilidades, vírus de computador e ataques digitais diretos ou indiretos, devem ser reportados imediatamente para a área segurança da Informação.

Mais detalhes devem ser observados no “Procedimento de Gestão de Suporte TI”.

## BYOD:

A empresa possui a “Norma de Gestão de BYOD” (Política para utilização de dispositivos dos próprios Colaboradores), publicada com diretrizes e controles bem definidos relacionada a esse tema.

## UTILIZAÇÃO DA REDE CORPORATIVA:

Não é permitido utilização equipamentos pessoais para acesso à rede corporativa, exceções devem ser avaliadas, justificadas e documentadas através do fluxo de exceções;

Toda máquina para acesso à rede corporativa deve possuir certificado digital;

Não é permitido utilizar qualquer tipo de conexão remota externas, nos equipamentos que estejam ao mesmo tempo conectados na rede corporativa (Esta prática pode expor as informações da empresa e/ou contaminar o ambiente corporativo com vírus).

Não é permitido a expansão da rede corporativa através de roteadores, switches, hubs, sem a autorização da equipe de REDES e Segurança da Informação;

Fornecedores e visitantes devem usar conexão própria para acesso à Internet ou rede segregada da rede corporativa (GUEST, visitantes).

## PROPRIEDADE INTELECTUAL:

Todos os bens materiais físicos ou lógicos, gerados ou desenvolvidos pelos colaboradores, terceiros, prestadores de serviço e parceiros, no exercício de suas atribuições, utilizando recursos tecnológicos da empresa, mesmo que fora do horário de trabalho, são de propriedade exclusiva da Brejeiro.

> **Ex.: Informações, documentos (físicos ou lógicos), criações, inventos, desenvolvimentos, aperfeiçoamentos ou outras melhorias feitas, armazenados, produzidos ou transformados.**

Todo usuário é responsável pela preservação da propriedade intelectual da organização, bem como pela observância e respeito à propriedade intelectual de terceiros, nos termos da legislação vigente, cabendo à responsabilização em casos de omissão, dolo ou culpa.

Todas as informações que pertençam à empresa, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

## SEGURANÇA DE ACESSOS (LÓGICO E FISÍCO):

Todo colaborador é responsável por todos os atos executados com seus acessos (físicos ou lógico), assim como todos os atos executados em sua estação de trabalho enquanto logado, visto que os acessos são únicos, pessoais e intransferíveis.

## GESTÃO DE ACESSOS FÍSICOS:

A empresa possui a “Norma de Gestão de Acessos Físicos publicada”, com diretrizes e controles bem definidos relacionada a esse tema.

## GESTÃO DE IDENTIDADES E ACESSOS LÓGICOS:

A empresa possui a “Norma de Gestão de Identidades e Acessos Lógicos publicada”, com diretrizes e controles bem definidos relacionada a esse tema.

## GESTÃO E CONFIGURAÇÃO DE SENHAS:

A empresa possui a “Norma de Gestão e Configuração de Senhas” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## SEGURANÇA DE DADOS:

Todas as informações da Brejeiro devem receber uma classificação, assim como um nível adequado de proteção, de acordo com o seu valor, grau de sigilo, sensibilidade e criticidade para o negócio.

Todas as informações da Brejeiro devem ser manuseadas e armazenadas somente em computadores corporativos e/ou nuvem privada oficiais da empresa.

Não é permito manusear, armazenar e transferir informações, sem autorização, para dispositivos ou meios de armazenamento externos, assim como ambientes de armazenamento em nuvens que não sejam da empresa (Dropbox, OneDrive, iCloud, Google Drive, dentre outros).

## CLASSIFICAÇÃO DA INFORMAÇÃO (DADOS):

A empresa possui a “Norma de Classificação da Informação” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## GESTÃO E SEGURANÇA DE DADOS (DLP):

A empresa possui a “Política de Gestão e Governança de Dados” e a “Norma de Gestão de DLP”, ambas publicadas, com diretrizes e controles bem definidos relacionada a esse tema.

## GESTÃO DE ATIVOS:

Os ativos associados com informações corporativas devem ser identificados e inventariados.

Para todo ativo, deve ser definido um Owner (responsável), independente do seu meio de acesso, seja em sistemas, servidor ou banco de dados, mantendo a proteção adequada de acordo com a grau de risco, assim como as aprovações corretas de acessos;

A empresa possui a “Norma de Gestão de Ativos” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## SEGURANÇA DE CLOUD (CLOUD SECURITY):

A empresa possui a “Norma de Gestão de Segurança em CLOUD” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## SEGURANÇA DE RECURSOS TECNOLÓGICOS:

É estritamente proibido a utilização de dispositivos vinculados à Tecnologia de Informação (servidores, banco de dados, roteadores, softwares de desenvolvimento etc.) que não sejam gerenciados e homologados pela área de TI ou segurança da informação;

Os recursos tecnológicos corporativos devem ter minimamente implementado:

- Todos os servidores devem ser monitorados constantemente para a eliminação de vulnerabilidades de segurança, bem como a aplicação de correções de segurança reportadas;
- Segregação de rede, seja esta física ou lógica, através dos mecanismos e tecnologias aplicáveis, assegurando a confidencialidade, integridade e disponibilidade das informações trafegadas;
- Softwares de antivírus em todas as estações de trabalho e servidores, com processos estabelecidos que garantam as atualização e execuções adequadas;
- Proteção de e-mails (Anti-spoofing, filtro de reputação, AntiSpam, Anti-phishing);
- Equipamentos que estabeleçam barreiras de segurança (Firewalls e WAF);

- Mecanismos de detecção de intrusos devem ser adotados em todas as comunicações da rede corporativa com o meio externo;
- Os computadores de usuários devem dispor de recursos de firewall pessoal, bem como configurações de segurança, a atualização de patches, visando à redução de chances de invasões, evasão de informações e/ou acessos não autorizados;

Controles tecnológicos devem ser implementados visando monitorar, proteger e minimizar os riscos associados às informações ou ativos de processamento, de modo a preservar suas propriedades de confidencialidade, integridade e disponibilidade. Estes controles devem atuar na prevenção, restrição, monitoração e detecção de incidentes de segurança (Ex. NOC e SOC).

Os relógios dos ambientes e sistemas corporativos, devem ser sincronizados com uma fonte de tempo precisa e única para todos;

## GESTÃO DE RISCOS:

### RISCOS TECNOLÓGICOS:

A empresa possui a “Norma de Gestão de Riscos Tecnológico” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

### RISCOS CORPORATIVOS (FORNECEDORES):

A empresa possui a “Norma de Gestão de Riscos Corporativos” e “Procedimento Conheça seu Parceiro”, ambas publicadas, com diretrizes e controles bem definidos relacionada a esse tema.

### RISCOS EM PROJETOS:

As diretrizes e controles relacionados à segurança da informação descritos nesta política ou derivadas, devem ser consideradas no gerenciamento de projetos relacionados a contratação ou desenvolvimento de novos produtos, sistemas ou serviços. Assim como, a equipe de Segurança da Informação deve ser envolvida para alinhamentos e avaliações durante as etapas dos projetos, de forma a assegurar que os riscos sejam conhecidos, gerenciados e mitigados.

## GESTÃO DE AMEAÇAS E VULNERABILIDADES:

A empresa possui a “Norma de Gestão de Ameaças e vulnerabilidades” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## CONFIGURAÇÕES DE SEGURANÇA E PATCHES:

A empresa possui o “Procedimento de Gestão de Configurações de Segurança e Patches” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## DESENVOLVIMENTO SEGURO:

O desenvolvimento de sistema seguro visa proteger a empresa de utilizar sistemas com códigos passíveis a exploração de vulnerabilidades e/ou códigos maliciosos, podendo gerar a empresa.

As equipes de desenvolvimento da empresa devem seguir as melhores práticas de desenvolvimento seguro, como exemplo OWASP e NIST.

A empresa possui a “Norma de Gestão de desenvolvimento Seguro” publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## CRIPTOGRAFIA:

Deve haver um processo de criptografia de disco em todos os notebooks e dispositivos móveis corporativos, para proteger quanto a confidencialidade das informações e possíveis vazamentos de dados derivados de perda ou roubo dos equipamentos.

Toda aplicação que contenha informações da empresa e esteja hospedada em ambiente externo deve suportar comunicação com protocolo seguro (https) e criptografia forte no tráfego dos dados;

Deve ser implementado mecanismos específicos de criptografia na transmissão de informações corporativas através da internet (Ex.: API's, serviços, comunicação com parceiros etc.), assim como as chaves criptográficas devem ser armazenadas de forma segura e centralizada em softwares de gerenciamento ou cofres de senhas corporativo; conforme descrito na "Norma de Gestão e Configuração de Senhas"

## GESTÃO DE LOGS E TRILHAS DE AUDITORIA:

Todos os sistemas que venham a ser considerados como críticos para o negócio devem possuir trilhas de auditoria habilitadas, devendo ser registradas todas as operações privilegiadas, início e finalização de acesso ao sistema, conexão e desconexão de dispositivos, tentativas de acesso não autorizadas, violação de dispositivos de segurança etc.

As informações dos registros de eventos (log) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.

A empresa possui a "Norma de Gestão de Logs e Trilhas de Auditoria" publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## MONITORAMENTO DE EVENTOS (SOC/NOC):

A empresa possui o "Procedimento de Monitoramento e Logs e Eventos de SI (SOC)" e o "Procedimento de Monitoramento e Logs e Eventos de TI (NOC)" ambos publicados, com diretrizes e controles bem definidos relacionada a esse tema.

## GESTÃO E RESPOSTAS A INCIDENTES:

A empresa possui a "Norma de Gestão de Incidentes" e "Procedimento de Respostas a Incidentes de SI, TI e Negócio", ambos publicados, com diretrizes e controles bem definidos relacionada a esse tema.

## TRATAMENTO DE FRAUDE:

Todas as ocorrências de fraudes ou suspeitas devem ser investigadas, registradas e tratadas de forma condizente à dimensão da situação.

Deve ser instituído um canal para denúncias no sentido de obter contribuições voluntárias para a identificação e a eliminação de potenciais fraudes ou desvios de comportamento identificadas pelos colaboradores, prestadores de serviço ou clientes.

## GESTÃO DE BACKUP E RESTORE:

A empresa possui a "Norma de Gestão de Backup e Restore" publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## CONTINUIDADE DE NEGÓCIO (GCN):

A empresa deve manter planos e processos que visam manter a empresa operacional, sem grandes impactos aos clientes, mesmo após um desastre, até o retorno à situação de normalidade, sempre alinhado às necessidades do negócio. Assim como devem ser revisados e testados periodicamente.

A empresa possui a "Norma de Gestão de Continuidade de Negócio GCN" publicada, com diretrizes e controles bem definidos relacionada a esse tema.

## CANAIS DE COMUNICAÇÃO E DENUNCIAS:

Devem ser estabelecidos canais de comunicação específicos, possibilitando aos colaboradores (funcionários e prestadores de serviço), os meios necessários à realização de denúncias sobre a não aderência aos princípios desta política ou outras situações que ponham em risco a segurança organizacional da empresa.

## VIOLAÇÃO E SANÇÕES:

Os princípios estabelecidos nesta política possuem total aderência da Alta Administração da Organização e devem ser observados por todos da Brejeiro, na execução de suas funções.

Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta política e derivadas.

Deve ser estabelecido procedimentos disciplinares formais para colaboradores, terceiros e prestadores de serviços, que venham a cometer infrações, violações ou incidentes graves de segurança, derivados ao não cumprimento das diretrizes descritas nesta política e derivadas, assim como a "Política de Código de ética e conduta".

São consideradas também violações a esta política as seguintes situações:

- Uso indevido e divulgação não autorizada de informações, segredos comerciais ou outras informações sem autorização formal;
- Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis, regulamentos internos e externos;
- Qualquer situação que exponha a Brejeiro a perdas financeiras ou de imagem, em decorrência da quebra da confidencialidade, integridade ou disponibilidade das suas informações ou das quais que detenham custódia.

Todos os colaboradores, terceiros e prestadores de serviço devem estar cientes de que o não cumprimento das diretrizes desta política implicará em sanções, sejam internas, administrativas, legais e/ou penais, dependendo do grau da infração. Para Terceiros e prestadores de serviços, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

Ao detectar uma violação, o usuário deve comunicar aos responsáveis pela Segurança da Informação imediatamente. Caso seja verificado que o colaborador não comunicou a infração, mesmo sabendo da sua existência, o mesmo pode ser considerado coautor da mesma e assim ser indiciado e sofrer sanções.

## PAPÉIS E RESPONSABILIDADES:

### COLABORADORES EM GERAL:

- Utilizar os recursos e serviços de tecnologia disponibilizados pela empresa de modo seguro, responsável, moral e ético;
- Notificar a área de Segurança da Informação sobre possíveis incidentes e violações de segurança que venha a ter conhecimento;
- Participar das campanhas, workshops e treinamentos de segurança; conhecer e praticar as diretrizes publicadas nas políticas de segurança

- Todo colaborador, deve observar e seguir as políticas, normas e procedimentos estabelecidas pela Brejeiro, sendo imprescindível a compreensão do papel da Segurança em suas atividades diárias.
- É de responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou causar a Brejeiro ou a terceiros, em decorrência da não obediência às diretrizes aqui referidas e caso seja desligado ou tenha seu contrato rescindido deverá devolver todas as informações da empresa que estiverem eventualmente em seu poder.

## GERENTES E GESTORES EM GERAL:

- Garantir que todos os colaboradores da empresa tenham ciência das diretrizes de segurança da informação presentes nesta Política e derivadas.
- Avaliar e aprovar os acessos requeridos de sua equipe.
- Revisar de forma periódica as identidades e os acessos que seus subordinados possuem atestando sua necessidade e/ou revogando quando não mais necessários.
- Revisar de forma periódica a Matriz de acessos de sua área.
- Informar o desligamento de colaboradores, prestadores de serviço ou parceiros que estão sob sua gestão direta no prazo máximo de 1 dia após o término da relação com eles.
- Alinhar os processos de desligamento tempestivo quando houver algum risco quanto à segurança das informações da empresa e/ou de nossos clientes.
- Informar a troca de área de colaboradores, prestadores de serviço ou parceiros que estavam sob sua gestão direta no prazo máximo de 1 dia após a mudança.

## EXECUTIVOS (ALTA GESTÃO):

- Assegurar que os objetivos de segurança da informação estão identificados, cumprem com os requerimentos da Brejeiro e estão integrados nos processos correspondentes da empresa;
- Prover o adequado direcionamento e suporte para as iniciativas de segurança da informação;
- Apoiar, difundir e alavancar o cumprimento das políticas e controles de segurança da informação através da organização, provendo os recursos humanos e orçamentários necessários.

## COMITE DE SEGURANÇA DA INFORMAÇÃO:

- Deliberar sobre os principais aspectos de segurança da informação, garantindo que os projetos e iniciativas sejam entendidos, avaliados e priorizados pela Alta Direção;
- Definir e coordenar a aplicação dos recursos humanos e orçamentários requeridos para cumprir com as políticas e controles de segurança da informação;
- Definir as prioridades para tratamento dos riscos identificados através da elaboração de planos de ação e, assegurar que eles sejam cumpridos conforme planejado;
- Apoiar e supervisionar as ações conduzidas em cumprimento às políticas de segurança da informação;

## EQUIPE DE SEGURANÇA DA INFORMAÇÃO (CYBER):

Estabelecer, por meio da definição de políticas, normas, procedimentos e controles, a integridade, disponibilidade e a confidencialidade das informações contidas nos ambientes da empresa, minimizando possíveis impactos e vulnerabilidades, reduzindo a ocorrência de incidentes de segurança que afetem os negócios da Brejeiro.

Respaldar as demais áreas da empresa para impulsionar os comportamentos corretos de segurança cibernética, realizar avaliações de segurança e impor correções para os riscos e vulnerabilidades de segurança cibernética

Desta forma, tem as principais atribuições:

- Governança e Gestão das Políticas, Normas e procedimentos relacionadas à SI;
- Gerir atividades de proteção, coordenar e comunicar eventos de segurança cibernética.
- Gestão e Detecção de Vulnerabilidades;

- Testes de Invasão periódicos;
- Promover campanhas de conscientização;
- Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- Resposta a Incidentes de Segurança;
- Avaliar requisitos de segurança em novos projetos;

## EQUIPE DE SUPORTE (GESTÃO DE ACESSOS E SERVICE DESK):

- Suporte e manutenção de máquinas;
- Gestão de acessos aos sistemas e ambientes da empresa;
- Gerir e publicar o inventário de sistemas, máquinas, matriz de acessos;
- Definir o Owner e criticidade de cada sistema, junto ao time de Compliance;
- Seguir e operacionalizar as diretrizes e normas corporativas, com ênfase nas abaixo:
- Norma de Gestão de Identidades de Acessos;
- Norma de Gestão de Acessos Físico;
- Norma de Gestão e Configuração de Senhas;
- Norma de Gestão de Suporte TI;

## EQUIPE DE INFRAESTRUTURA / PRODUÇÃO:

- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de informação sob sua responsabilidade e/ou custódia;
- Estabelecer e manter atualizado o inventário de ativos de informação (sob sua responsabilidade e/ou custódia), recursos e seus respectivos proprietários;
- Controlar as alterações executadas nos ativos de TI assegurando que estas sejam analisadas criticamente e testadas, para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
- Tratar adequadamente os riscos e vulnerabilidades identificados nos ativos de informação e processos sob sua responsabilidade e/ou custódia.

## OWNER DOS SISTEMAS:

- Avaliar e aprovar os acessos requeridos aos sistemas / ambientes sob sua responsabilidade.
- Definir formalmente o seu substituto para efetuar as atividades na sua ausência.
- Governança e Gestão das Políticas, Normas e procedimentos relacionadas à SI;
- Gerir atividades de proteção, coordenar e comunicar eventos de segurança cibernética.
- Gestão e Detecção de Vulnerabilidades;
- Testes de Invasão periódicos;
- Promover campanhas de conscientização;
- Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- Resposta a Incidentes de Segurança;
- Avaliar requisitos de segurança em novos projetos;

## EXCEÇÕES:

Qualquer exceção a essas regras descritas nesta política deverá ser avaliada junto ao time de segurança da informação, e formalizado via fluxo de exceção à política.

Todas as exceções devem ser revisadas (passar por todo o fluxo novamente) pelo menos uma vez ao ano.

## VIGÊNCIA E REVISÃO:

Esta norma entra em vigor a partir da data de sua aprovação e sua revisão deve ocorrer no período máximo de 12 meses, ou sempre que se fizer necessária.

## CONTROLE DE VERSÕES:

| Item | Data | O que foi alterado? | Responsável |
|---|---|---|---|
| v.1.0 | 10/08/2024 | Primeira versão do documento | Fabiano Caetano |
| v.1.0 | 10/08/2024 | Revisão do documento | Carla Maniezio |
| v.1.0 | 10/08/2024 | Aprovação | Diretoria |

**Data de Publicação: 10/08/2024.**