POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

2. INTRODUÇÃO 3
3. OBJETIVO 3
4. PÚBLICO-ALVO 3
5. DIRETRIZES GERAIS 4
6. CONDUTA EM SEGURANÇA DA INFORMAÇÃO 6
7. ACESSO FÍSICO ÀS DEPENDÊNCIAS DA LOJACORR 8
8. ARMAZENAMENTO DE INFORMAÇÕES 10
9. USO DA INTERNET 11
10. USO DO CORREIO ELETRÔNICO 12
11. USO DE DISPOSITIVOS MÓVEIS 13
12. CLASSIFICAÇÃO DA INFORMAÇÃO 15
13. DOCUMENTOS DE REFERÊNCIA 17
14. CONCEITOS E DEFINIÇÕES 17
15. GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO 18
16. SUPORTE PARA A IMPLEMENTAÇÃO DO SGSI 19
17. VALIDADE E GESTÃO DE DOCUMENTOS 19
18. CASOS OMISSOS 19
19. INTELIGÊNCIA ARTIFICIAL 19
20. SISTEMAS TERCEIROS 21
21. ACOMPANHAMENTO E REVISÃO 22
22. DISPOSIÇÕES FINAIS 23
23. TERMO DE RECEBIMENTO E CIÊNCIA 23

2. INTRODUÇÃO

2.1. A Lojacorr através da sua Diretoria Executiva e Conselho de Administração formaliza o seu comprometimento em garantir a segurança das informações geradas e custodiadas pela organização, preservando a sua confidencialidade, integridade e disponibilidade.

2.2. Através do seu SGSI (Sistema de Gestão de Segurança da Informação) a Lojacorr estabelece, em seus processos organizacionais, rigoroso controle para proteger as informações contra diversas ameaças, tais como, vazamento, modificação, destruição, acesso não autorizado, indisponibilidade, entre outras.

2.3. Este sistema tem como diretriz principal a Política de Segurança da Informação (PSI), e para que a Lojacorr consiga alcançar o resultado de proteger seus ativos essas regras devem ser cumpridas por todos.

3. OBJETIVO

3.1 Estabelecer os princípios que regulamentam a segurança da informação na Lojacorr, visando garantir a confidencialidade, integridade e disponibilidade das informações geradas e custodiadas pela Lojacorr.

3.2 Determinar o comportamento aceitável dos usuários em relação aos recursos disponibilizados e ao uso das informações geradas e/ou custodiadas pela Lojacorr, como:

a) o acesso físico às instalações;
b) o acesso lógico aos sistemas e serviços;
c) o armazenamento de informações lógicas e físicas;
d) uso do da Internet;
e) uso do correio eletrônico corporativo;
f) uso de dispositivos móveis;
g) definir os critérios para classificação das informações.

4. PÚBLICO-ALVO

4.1 Esta política é uma norma interna e se aplica a todos os colaboradores, prestadores de serviço, Unidades de Negócios, Corretoras da Rede e fornecedores que venham a ter acesso e/ou utilizam as informações, os recursos de Tecnologia da Informação Corporativa e/ou demais ativos tangíveis ou intangíveis da Lojacorr.

5. DIRETRIZES GERAIS

5.1. **Patrimônio:** As informações e recursos tecnológicos disponibilizados pela Lojacorr são considerados patrimônio e devem ser protegidos, considerando os requisitos do negócio e os riscos envolvidos;

5.2. **Acesso à Informação:** O acesso às informações, independente do meio em que estejam armazenadas, devem ser disponibilizadas apenas aos usuários autorizados.

5.3. **Responsabilidades:**

5.3.1. **Área de infra e segurança da informação**: Quanto à gestão de segurança da informação, serão responsabilidades específicas dessa área:

a) Zelar pela eficácia dos controles de Segurança da Informação utilizados e informar aos gestores e demais interessados os riscos residuais;

b) Configurar os recursos tecnológicos concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação;

c) Gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes; para as trilhas geradas e/ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências;

d) Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

e) Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

f) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos;

g) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas internas da organização;

h) 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, responsável pelo uso da conta;

i) Proteger continuamente todos os ativos de informação da Lojacorr 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;

j) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas;

k) Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Lojacorr;

l) Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento funcional, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos da Lojacorr.

m) Avaliar se as informações sobre de segurança da informação, eventos que violem essa política ou que coloquem em risco a segurança das informações ou dos recursos tecnológicos da Lojacorr que receber dos usuários configuram são um incidente e se confirmado, encaminhar todos os fatos e evidências ao DPO (dpo@redelojacorr.com.br).

5.3.2 **Responsável de segurança da informação**: São de sua responsabilidade:

a) Promover cultura de segurança da informação e comunicações no âmbito de suas atribuições dentro da Lojacorr;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de segurança da informação;

d) Coordenar o Comitê de Segurança da Informação e a Equipe Técnica de Segurança da Informação;

e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

f) Definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

g) Propor normas internas relativas à segurança da informação.

5.3.3 **Equipe técnica de segurança da informação**: É de responsabilidade específica desta equipe:

a) Propor metodologias e processos específicos para a segurança da informação, como classificação da informação e avaliação de risco;

b) Propor e apoiar iniciativas que visem à segurança dos ativos de informação;

c) Auxiliar na publicação e promoção da Política de Segurança da Informação, das normas, e procedimentos específicos decorrentes, aprovados pelo Comitê de Segurança da Informação;

d) Promover a conscientização dos usuários em relação à relevância da segurança da informação, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;

e) Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
f) Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação;
g) Buscar alinhamento das práticas de segurança da informação com as diretrizes corporativas da Lojacorr.

5.3.4 **Comitê de segurança da informação**: Compete ao Comitê de Segurança da Informação:
a) Assessorar na implementação das ações de segurança da informação;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
c) Propor alterações e revisar periodicamente a Política de Segurança da Informação, em conformidade com a legislação existente sobre o tema;
d) Propor, aprovar, alterar e revisar procedimentos internos de segurança da informação.

5.3.5 **Gestor de área**
a) Gerenciar o cumprimento da PSI, normas e instruções por parte dos usuários que lhe são subordinados;
b) Identificar as ameaças significativas e a exposição da informação na sua área;
c) Promover a conscientização pela segurança da informação na sua área;
d) Monitorar os controles de segurança da informação e realizar uma análise crítica dos incidentes de segurança da informação na sua área;
e) Reportar qualquer sugestão para melhoria, correção ou ameaça à PSI ao CSI;
f) Solicitar o auxílio do CSI quando necessário;

6. CONDUTA EM SEGURANÇA DA INFORMAÇÃO

6.1 RESPONSABILIDADE DOS USUÁRIOS

6.1.1 Conhecer e cumprir as orientações definidas na política de segurança da informação da Lojacorr.

6.1.2 Reportar ao gestor de sua área as melhorias, sugestões e ameaças à PSI.

6.1.3 Zelar pelas informações a que tenham acesso, independente do meio em que estejam armazenadas.

6.1.4 Informar incidentes de segurança da informação à área de infra e segurança da informação, pela central de atendimento (abrir chamado para a área de infraestrutura), bem como qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos tecnológicos da Lojacorr;

6.1.5 Recomendar mecanismos de proteção para a área de segurança da informação.

6.1.6 Utilizar as informações e recursos disponibilizados pela Lojacorr respeitando a legislação vigente, direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade, proteção de propriedade intelectual e a regulamentação interna.

6.1.7 Todos os colaboradores e prestadores de serviços devem assinar um Termo de Sigilo e Confidencialidade com a Lojacorr se comprometendo em utilizar os recursos e informações da organização de forma adequada, respeitando os critérios definidos na política de segurança da informação.

6.1.8 Cada colaborador é responsável pela segurança das informações, principalmente daquelas que estão sob sua responsabilidade.

6.1.9 Assinar o "Termo de Ciência e Concordância" no ato de recebimento da Política de Segurança da Informação e Privacidade da Lojacorr, formalizando o conhecimento e o aceite integral das disposições estabelecidas no referido instrumento, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

6.1.10 Responder pela inobservância da Política de Segurança da Informação e Privacidade, normas e procedimentos de segurança.

6.2 MESA LIMPA E TELA LIMPA

6.2.1 Manter sua mesa de trabalho limpa, sem deixar expostos documentos ou mídias removíveis contendo informações confidenciais.

6.2.2 Efetuar logout ou bloquear sua estação de trabalho sempre que se ausentar da estação de trabalho.

6.3 INFORMAÇÕES IMPRESSAS

6.3.1 Ao imprimir documentos contendo informações confidenciais o usuário deve permanecer próximo à impressora.

6.3.2 O descarte de documentos contendo informações confidenciais deve seguir o procedimento previsto no Quadro de tratamento da informação.

6.4 NÃO É PERMITIDO

6.4.1 Utilizar a marca da Lojacorr sem autorização.

6.4.2 Reutilizar documentos impressos contendo informações confidenciais.

6.4.3 Copiar ou emprestar softwares desenvolvidos ou adquiridos pela Lojacorr sem a autorização formal da Diretoria Executiva.

6.4.4 Conversar sobre assuntos confidenciais relacionados à Lojacorr em locais públicos.

6.4.5 Deixar recados com assuntos confidenciais relacionados à Lojacorr em secretárias eletrônicas.

6.4.6 Reproduzir documentos contendo informações da Lojacorr sem autorização do responsável pela informação.

6.4.7 Alimentar-se próximo ou sob os equipamentos.

7. ACESSO FÍSICO ÀS DEPENDÊNCIAS DA LOJACORR

7.1 IDENTIFICAÇÃO

7.1.1 A identificação é fornecida e controlada pela administração do condomínio.

7.1.2 A identificação de visitante deverá ser devolvida na saída das dependências do Condomínio.

7.1.3 Os visitantes devem ser instruídos em relação às regras de acesso às dependências da Lojacorr no momento da sua identificação.

7.2 ACESSO À SEDE DA LOJACORR

7.2.1 O acesso, a permanência e a circulação nas dependências da Lojacorr serão permitidos somente às pessoas autorizadas e com uso de identificação em local visível. O acesso de visitante e do colaborador que o acompanha deve ser registrado pela recepcionista da Lojacorr.

7.2.2 As dependências da Lojacorr são monitoradas por câmeras.

7.2.3 O acesso às áreas críticas é restrito a colaboradores autorizados. O acesso de fornecedores e prestadores de serviço à essas áreas deve ser registrado pela área de infra e segurança da informação.

7.2.4 O acesso ao datacenter será protegido por sistema com controle por biometria. Somente colaboradores da área de infra e segurança da informação e as pessoas que forem definidas pelo CSI terão acesso.

7.2.5 O acesso dos colaboradores (pessoas físicas ou jurídicas) cujo contrato de trabalho houver sido rescindido, por qualquer motivo, às instalações da Lojacorr ficará restrito às áreas de acesso público, pois sua credencial, o uso de equipamentos e acessos físicos e lógicos são revogados.

7.3 EQUIPAMENTOS DA SEDE

7.3.1 A entrada e saída de equipamentos de propriedade da Lojacorr que estiverem na sede deve ser autorizada e registrada junto a área de infra e segurança da informação.

7.3.2 Devolução de computadores pelos colaboradores demitidos para sede, deve ocorrer dentro de 48h corridas (contadas do recebimento do código dos correios).

7.3.3 Os equipamentos que armazenam informações confidenciais, como, por exemplo, o notebook de um colaborador que estiver trabalhando na sede, deve ser posicionado de forma a não permitir acessos indevidos às informações.

7.3.4 Os arquivos físicos contendo informações confidenciais devem ter mecanismos de proteção física e seu acesso deve ser restrito aos usuários autorizados.

7.4 ACESSO LÓGICO

7.4.1 O acesso lógico aos sistemas e serviços, disponibilizados pela Lojacorr, é realizado por meio de autenticação.

7.4.2 Os logins e senhas são pessoais e intransferíveis.

7.4.3 O acesso aos sistemas e serviços é permitido somente para execução das atividades profissionais relacionadas à Lojacorr.

7.4.4 Os acessos aos sistemas e serviços podem ser monitorados pela Lojacorr.

7.4.5 A liberação de acesso deve observar a Política de classificação da informação da Lojacorr e os privilégios necessários à função do usuário.

7.4.6 Os recursos e serviços da rede corporativa, quando possível de serem acessados remotamente, poderão ser acessados somente por VPN (Virtual Private Network). Este é o dispositivo de segurança utilizados para manter os acessos remotos criptografados;

7.4.7 As exceções devem ser explícitas e formalizadas entre as partes.

7.5 BLOQUEIO

7.5.1 O acesso do usuário será bloqueado nas seguintes situações:

a) Quando ocorrer o desligamento, férias e ou afastamento por doença do usuário.
b) Quando houver indício de uso inadequado dos sistemas e serviços.

7.6 POLÍTICA DE SENHAS

7.6.1 A senha deve ter o mínimo 8 caracteres, devendo conter letras, números e caracteres especiais.

7.6.2 As senhas dos softwares desenvolvidos ou contratados pela Lojacorr devem, preferencialmente, expirar a cada 3 (três) meses.

7.6.3 A reutilização de senhas não é permitida.

7.7 ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO

7.7.1 Os direitos de acesso dos usuários devem ser revisados anualmente ou sempre que ocorrerem mudanças relacionadas à função dos usuários.

7.7.2 Os direitos de acesso dos usuários com privilégios administrativos devem ser revisados semestralmente ou quando ocorrerem mudanças de função desses usuários.

7.8 **CONEXÃO NA REDE**

7.8.1 Somente equipamentos autorizados pela área de infra e segurança da informação terão acesso aos sistemas e serviços da sede da Lojacorr.

7.9 **ACESSO REMOTO**

7.9.1 O acesso remoto aos sistemas e serviços é permitido somente com autorização da área de infra e segurança da informação.

7.10 **NÃO É PERMITIDO**

7.10.1 Compartilhar credenciais (usuário e senha) de acesso aos sistemas e serviços da Lojacorr.

7.10.2 Manter senhas anotadas em qualquer meio que coloque em risco a sua descoberta.

8. ARMAZENAMENTO DE INFORMAÇÕES

8.1 **GERAL**

8.1.1 O armazenamento de informações nos recursos tecnológicos disponibilizados pela Lojacorr é permitido apenas para informações relacionadas às atividades profissionais de interesse da organização.

8.1.2 A utilização de espaço em disco nos equipamentos da Lojacorr será monitorada.

8.1.3 Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade.

8.1.4 O armazenamento de arquivos, dados e informações deve ocorrer obrigatoriamente na estrutura Workspace Google da Lojacorr.

8.1.5 A Lojacorr não fará backup de arquivos salvos fora da estrutura Workspace Google. Por isso, ao salvar seus arquivos fora dessa estrutura, o usuário pode perder informações e dados, e a proteção de dados pode ser violada

8.2 **MÍDIAS REMOVÍVEIS**

8.2.1 O uso de mídias removíveis é permitido somente a usuários autorizados.

8.3 **DOCUMENTOS FÍSICOS**

8.3.1 Os documentos impressos devem ser armazenados em locais com acesso restrito aos usuários que necessitem da informação.

8.4 **NÃO É PERMITIDO**

8.4.1 Armazenar informações da Lojacorr em equipamentos ou mídias particulares.

8.4.2 Armazenar nos equipamentos disponibilizados pela Lojacorr materiais que impliquem na violação da legislação vigente ou regulamentações internas, tais como: arquivos de música, vídeos que não sejam de uso de atividades de trabalho, de conteúdo pornográfico, homofóbico, obsceno, fraudulento, difamatório e racista. Todo e qualquer material citado acima que for encontrado na rede ou no equipamento do usuário, será excluído imediatamente sem prévia autorização do usuário.

8.4.3 Salvar documentos na área de trabalho dos computadores fornecidos pela Lojacorr.

9. USO DA INTERNET

9.1 **GERAL**

9.1.1 A utilização do serviço de internet disponibilizado na sede Lojacorr será monitorada.

9.1.2 O serviço de internet, disponibilizado pela Lojacorr em sua rede corporativa, deve ser utilizado para atividades profissionais relacionadas ao negócio da Lojacorr.

9.1.3 Somente equipamentos autorizados pela área de Infraestrutura da Lojacorr podem utilizar o serviço de internet da Lojacorr.

9.1.4 O uso de ferramentas e/ou serviços de troca de mensagens é permitido somente com autorização do Comitê de segurança da informação e para fins profissionais.

9.1.5 A Lojacorr poderá monitorar e registrar os acessos à rede mundial de computadores do usuário que estiver utilizando os recursos (notebook, rede corporativa, etc) fornecidos por ela.

9.2 **NÃO É PERMITIDO**

9.2.1 Visualizar, armazenar, divulgar e transmitir qualquer material de conteúdo ilícito, tais como racismo, pedofilia e pornografia, ou qualquer material que defenda atividades ilegais.

9.2.2 Acessar e/ou propagar deliberadamente qualquer tipo de conteúdo malicioso (por ex. propaganda enganosa, promessas, pirâmides, entre outros).

9.2.3 Participar de qualquer discussão pública sobre os negócios da Lojacorr (por exemplo: estratégias comerciais, procedimentos administrativos, detalhes de acordos com seguradoras e demais assuntos cujo sigilo deve ser observado conforme previsto no Acordo de Sigilo assinado por todos, entre outros) por meio de salas de chat, grupos de discussão, redes sociais ou qualquer outro tipo de fórum público sem autorização prévia.

9.2.4 Realizar download de softwares.

9.2.5 Utilizar redes sociais corporativas da Lojacorr fins de entretenimento.

9.2.6 Utilizar disco virtual por meio rede corporativa da Lojacorr.

9.2.7 Enviar, copiar ou abrir documentos provenientes de chat quando estiver utilizando rede corporativa (VPN, internet da sede, etc) da Lojacorr. Essa proibição não se aplica ao google chat da Lojacorr.

10. USO DO CORREIO ELETRÔNICO

10.1 GERAL

10.1.1 O correio eletrônico disponibilizado pela Lojacorr deve ser utilizado somente para troca de informações relacionadas às atividades profissionais.

10.1.2 O e-mail disponibilizado pela Lojacorr é de uso pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

10.1.3 O uso do correio eletrônico disponibilizado pela Lojacorr pode ser auditado.

10.1.4 O tamanho de arquivos anexados aos e-mails é limitado a 10MB.

10.2 ARMAZENAMENTO DE E-MAILS

10.2.1 Somente recursos tecnológicos disponibilizados pela Lojacorr podem ser utilizados para armazenar mensagens eletrônicas da empresa.

10.3 NÃO É PERMITIDO

10.3.1 Instalar o correio eletrônico particular nos equipamentos da Lojacorr.

10.3.2 Utilizar e-mail particular para enviar mensagens relacionadas ao negócio da Lojacorr.

10.3.3 Divulgar o e-mail fornecido pela Lojacorr para recebimento de mensagens particulares.

10.3.4 Executar arquivos anexados ou clicar em links de e-mails recebidos cujo remetente e/ou origem seja suspeita.

10.3.5 Utilizar qualquer mecanismo que possibilite alterar informações sobre o remetente da mensagem.

10.3.6 Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Lojacorr;

10.3.7 Enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

10.3.8 Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

10.3.9 Produzir, armazenar, transmitir ou divulgar mensagem que:

a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Lojacorr;
b) contenham ameaças eletrônicas, como: spam, mail bombing, vírus;
c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
d) vise obter acesso não autorizado a outro computador, servidor ou rede;
e) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
f) vise burlar qualquer sistema de segurança;
g) vise vigiar secretamente ou assediar outro usuário;
h) vise acessar informações confidenciais sem explícita autorização do proprietário;
i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
j) inclua imagens criptografadas ou de qualquer forma mascaradas;
k) contenha veiculação/visualização de vídeos, fotografias e imagens associadas ou de qualquer forma relacionadas a pornografia, ou ainda relacionadas a ideias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou quaisquer outras formas de discriminação.
l) Conteúdo ilícito. Entretenimentos, correntes e assuntos impertinentes ao trabalho.
m) Materiais aos quais se aplicam as leis de direitos autorais e cujo uso não tenha sido autorizado por seu proprietário.
n) Informações que prejudiquem a imagem da Lojacorr.
o) Mensagens que configure assédio sexual ou moral.
p) Músicas, vídeos ou animações que não sejam de interesse do negócio da Lojacorr.

11. USO DE DISPOSITIVOS MÓVEIS

11.1 CONTROLE

11.1.1 Todo dispositivo móvel disponibilizado pela Lojacorr deve ser registrado e controlado.

11.1.2 Cada colaborador receberá um notebook para uso durante a prestação de serviços, que ficará sob sua responsabilidade.

11.1.3 Os usuários devem assinar um termo de responsabilidade quando receberem o dispositivo móvel da Lojacorr.

11.1.4 Os colaboradores deverão utilizar os dispositivos móveis fornecidos pela Lojacorr na sua atividade profissional.

11.1.5 Os usuários devem devolver os dispositivos móveis no momento do desligamento ou em até 48h corridas (contadas do recebimento do código de envio dos correios).

11.1.6 Em caso de perda, roubo, furto ou extravio dos dispositivos móveis fornecidos pela Lojacorr, o responsável deve informar imediatamente a área de segurança da informação para que sejam tomadas as providências cabíveis.

11.1.7 Os dispositivos móveis da Lojacorr são passíveis de inventário e verificação de softwares instalados.

11.1.8 Os colaboradores não possuem a propriedade do equipamento, sendo terminantemente proibido o empréstimo, aluguel ou a cessão deste a terceiros não autorizados.

11.1.9 Não é permitido aos colaboradores utilizarem na sua atividade profissional softwares não licenciados ou que não sejam autorizados pela área de infra e segurança da informação.

11.1.10 Todos os equipamentos disponibilizados pela Lojacorr aos colaboradores para prestação de seus serviços, são de responsabilidade deles quanto seu uso adequado, proteção e guarda, conforme previsto no Termo de Responsabilidade e Recebimento de Equipamento Portátil assinado na ocasião do recebimento do equipamento.

11.1.11 Os colaboradores deverão observar as normas para utilização dos equipamentos recebidos da Lojacorr constantes na Política de utilização de equipamentos, código de conduta e, também, no caso de trabalho remoto, as instruções constantes na Política de Teletrabalho.

11.2 CONFIGURAÇÃO

11.2.1 Os equipamentos móveis disponibilizados pela Lojacorr devem possuir:

a) Sistema operacional e aplicações com a versão disponível mais recente. Antivírus atualizado.

b) Senhas de acesso.

c) Somente softwares e recursos homologados pela Lojacorr devem ser instalados e/ou utilizados nos dispositivos móveis da empresa.

11.3 CONEXÃO

11.3.1 A conexão de dispositivos móveis particulares aos recursos da Lojacorr deve ser autorizada pela área de infra e segurança da informação.

11.3.2 A liberação de acesso dos dispositivos móveis deve seguir os critérios definidos na norma de acesso lógico.

11.3.3 Os dispositivos autorizados a utilizar os recursos tecnológicos da Lojacorr devem ser registrados pela área de infra e segurança da informação.

11.4 **ARMAZENAMENTO DE INFORMAÇÕES**

11.4.1 O armazenamento de informações em dispositivos móveis deve seguir os critérios definidos na norma de armazenamento de informações.

11.4.2 Não é permitido armazenar informações da Lojacorr em dispositivos móveis particulares, mas caso isso ocorra, o dispositivo móvel particular poderá ser periciado a qualquer momento pela Lojacorr.

11.4.3 Não armazenar documentos na área de trabalho do notebook disponibilizado pela Lojacorr.

11.4.4 A guarda das informações armazenadas nos dispositivos móveis disponibilizado pela Lojacorr é de responsabilidade do usuário que tem a custódia do dispositivo.

11.5 **MANUTENÇÃO**

11.5.1 As informações armazenadas nos dispositivos móveis da Lojacorr devem ser descartadas antes do envio para manutenção externa.

11.5.2 Somente a área de infra e segurança da informação poderá realizar manutenções e/ou alterações no software de antivírus.

11.6 **TRANSPORTE**

11.6.1 Ao transportar dispositivos móveis, o usuário deve zelar pelo dispositivo deixando-o sempre em local seguro.

12. CLASSIFICAÇÃO DA INFORMAÇÃO

12.1 **GERAL**

12.1.1 Os usuários devem ter acesso somente às informações que sejam necessárias ao desenvolvimento de suas atividades profissionais na Lojacorr.

12.1.2 Um inventário de ativos associado às informações e dos recursos disponibilizados pela Lojacorr deve ser mantido atualizado.

12.1.3 No inventário deve ser indicado o proprietário do ativo e sua classificação.

12.2 **CLASSIFICAÇÃO**

12.2.1 Toda informação gerada ou custodiada pela Lojacorr deve ser classificada de acordo com o nível de sensibilidade que representa para o negócio.

12.2.2 A classificação deve considerar o valor da informação, os requisitos legais, a sensibilidade, a criticidade, a vida útil da informação, a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o negócio.

12.2.3 A classificação da informação deve ser realizada no momento em que for gerada ou inserida nos processos da Lojacorr ou no momento em que for identificado que ainda não foi classificada.

12.3.4 Os seguintes níveis devem ser considerados na classificação da informação na Lojacorr:

a) Confidencial: Informações que requerem um tratamento especial e cuja divulgação não autorizada ou acessos indevidos podem gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégias da organização.

b) Restrita: Informações restritas que devem ser divulgadas a determinados grupos, áreas ou cargos, podendo conter público interno e/ou externo à organização.

c) Pública: Informações que podem ou devem ser divulgadas para público interno e/ou externo.

12.3.5 O proprietário da informação deve ser definido no momento da criação/recebimento da informação.

12.3.6 O proprietário da informação ou colaborador delegado por ele é responsável pela classificação das informações e definição de grupos de acesso.

12.3.7 Toda informação não classificada é considerada confidencial.

12.3 RECLASSIFICAÇÃO

12.3.1 Somente o proprietário da informação ou colaborador delegado por ele pode reclassificar informações.

12.3.2 A reclassificação deve ocorrer quando forem identificadas classificações indevidas, mudanças que impactem a sensibilidade as informações durante seu ciclo de vida ou quando ocorrer o fim do ciclo de vida da informação.

12.4 RÓTULOS

12.4.1 Toda informação deve ter rótulos indicando de forma clara a sua classificação.

12.4.2 A responsabilidade por incluir rótulo nas informações/recursos é do seu proprietário ou colaborador delegado por ele.

12.4.3 Os documentos e recursos que contenham informações de diferentes níveis de classificação devem ser classificados e rotulados de acordo com o nível mais restritivo existente em seu conteúdo.

12.4.4 A classificação de informações divulgadas verbalmente, sem uso de material escrito, deve ser informada pelo responsável no momento da sua divulgação.

12.5 TRATAMENTO DE INFORMAÇÕES

12.5.1 As informações de clientes, custodiadas pela Lojacorr, devem ser tratadas conforme nível de criticidade e sensibilidade definido pelo cliente, documentados em acordos ou contratos.

12.5.2 Todos os usuários devem comunicar ao proprietário da informação ou a área de segurança da informação a inexistência ou inconsistência na classificação da informação.

12.5.3 Um quadro de tratamento da informação deve ser elaborado e mantido atualizado.

12.5.4 Todos os usuários devem tratar as informações considerando sua classificação e o quadro de tratamento das informações.

12.6 **DIVULGAÇÃO**

12.6.1 Somente a Assessoria de Comunicação pode divulgar informações oficiais da empresa classificadas como públicas.

13. DOCUMENTOS DE REFERÊNCIA

Norma ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;
ISO/IEC 27000, Information technology - Security techniques - Information security management.
ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação – Técnicas de Segurança – Código de práticas para controles de segurança da informação.
ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação;
ABNT NBR ISO 31000:2009 - Gestão de riscos — Princípios e diretrizes
ABNT NBR ISO/IEC 31010:2012 Gestão de riscos — Técnicas para o processo de avaliação de riscos.
Código de conduta da Lojacorr

14. CONCEITOS E DEFINIÇÕES

Áreas Críticas: Áreas mapeadas pela área de infra e segurança da informação como importantes para segurança da Lojacorr.
Ativo de Informação: é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos;
Confidencialidade: as informações devem ser divulgadas apenas a indivíduos, entidades ou processos autorizados;
Conformidade: cumprimento de um requisito legal ou regulatório relacionado à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Lojacorr;
Controle de Acesso: são restrições ao acesso às informações de um sistema exercidas pela gerência de segurança da informação das entidades relacionadas à Lojacorr;

Custódia: consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

Direito de Acesso: é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

Disponibilidade – propriedade de estar disponível e utilizável quando necessário e autorizado. [ISO/IEC 27000:2014]

Ferramentas: é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PSI;

Informação: reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;

Incidente de Segurança da Informação: evento decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;

Integridade - características das informações que somente são alteradas somente por pessoas da forma permitida.

Recursos Tecnológicos: Todos os equipamentos da Lojacorr utilizados no trabalho pelos colaboradores, como, por exemplo, notebooks, celulares, impressoras, etc;

Rede Corporativa: É a Rede interna da Lojacorr, o notebook se conecta a ela quando ele estiver fisicamente na sede conectado na rede ou em qualquer local utilizando a VPN.

Risco de Segurança da Informação: riscos associados à violação da confidencialidade, integridade e disponibilidade das informações da Lojacorr nos meios físicos e digitais.

Segurança da Informação: conjunto de ações e controles com objetivo de garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos da Lojacorr;

SGSI - Sistema de gestão da segurança da informação - sistema de gestão que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.

Tecnologia da Informação: Atividades e soluções que são feitas através de recursos tecnológicos, como por exemplo, softwares, integração entre softwares, entre outros.

Usuário: Qualquer pessoa que possua login e senha do Broker One, seja Colaborador da Lojacorr, Colaborador das Unidades ou Corretoras da Rede, sócios, prepostos, terceiros etc.

15. GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

15.1 Os objetivos gerais para a gestão de segurança da informação são os seguintes:

a) Preservar a confidencialidade, integridade e disponibilidade das informações geradas e custodiadas pela organização.
b) Conhecer os riscos de segurança da informação no processo do escopo do SGSI em relação ao negócio da Lojacorr e realizar o tratamento dos riscos identificados.
c) Aumentar o nível de maturidade da Lojacorr em relação ao tema Segurança da Informação.

16. SUPORTE PARA A IMPLEMENTAÇÃO DO SGSI

16.1 A Diretoria Executiva declara que a implementação do SGSI e seu contínuo aprimoramento serão suportadas pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como atender todos os requisitos identificados.

17. VALIDADE E GESTÃO DE DOCUMENTOS

17.1 Este documento é válido a partir da data de sua emissão.
17.2 O proprietário do documento é a área de segurança da informação, que deve verificar e, se necessário, atualizar o documento anualmente.

18. CASOS OMISSOS

18.1 Os casos omissos serão avaliados pelo Comitê de Segurança da Informação para posterior deliberação.
18.2 As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da organização adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da organização.

19. INTELIGÊNCIA ARTIFICIAL

19.1. Governança e Responsabilidade

19.1.1 A Lojacorr deverá formar um um comitê permanente que será responsável pela supervisão das práticas de IA, garantindo conformidade com esta política.

19.1.2 A Área que utilizar IA ou pretende utilizar IA em qualquer projeto deve designar um colaborador que ficará responsável por comunicar o comitê e garantir a aderência do projeto/utilização às diretrizes de segurança e privacidade

19.2. Privacidade e Proteção de Dados

19.2.1 No processo de anonimização de Dados deve-se garantir que todos os dados utilizados para treinamento e operação de IA sejam anonimizados para proteger a privacidade dos indivíduos.

19.3 Segurança Cibernética

19.3.1 A área de Tecnologia da Lojacorr é responsável por **:**

a) Implementar e garantir medidas de segurança robustas para proteger os sistemas de IA contra ameaças cibernéticas, incluindo firewalls, criptografia e monitoramento contínuo;

b) Implementar sistemas de monitoramento contínuo para detectar e responder a anomalias e ameaças aos sistemas de IA.

19.3.2 O Colaborador/Parceiro que utilizar sistemas de IA é responsável por:

a) Garantir que todos os sistemas de IA utilizados sejam mantidos atualizados com os patches de segurança mais recentes.;

b) Manter transparência sobre como e por que os sistemas de IA estão sendo utilizados, incluindo a finalidade e os dados envolvidos;

c) Garantir que os sistemas de IA sejam explicáveis, permitindo que as decisões tomadas pelos algoritmos possam ser compreendidas e auditadas por humanos;

d) Garantir que todos os dados utilizados para treinamento e operação de IA sejam anonimizados para proteger a privacidade dos indivíduos;

e) Obter consentimento explícito dos indivíduos (titulares de dados) cujos dados forem utilizados, antes de utilizar seus dados em sistemas de IA;

f) Implementar procedimentos para identificar e mitigar possíveis vieses nos algoritmos de IA;

g) Assegurar que os sistemas de IA sejam utilizados de maneira ética e não discriminatória, respeitando os direitos e a dignidade de todas as pessoas.

19.3.3 As áreas de Controles Internos, Tecnologia e análises de dados devem:

a) verificar se todos os sistemas de IA utilizados pelos colaboradores da Lojacorr estão em conformidade com as leis e regulamentos aplicáveis, incluindo leis de proteção de dados e privacidade.

b) Realizar auditorias regulares para verificar a conformidade com esta política e com as normas legais.

19.4 Resposta a Incidentes

19.4.1 Plano de Resposta a Incidentes**:** Desenvolver e manter um plano de resposta a incidentes específico para IA, incluindo procedimentos para a contenção, erradicação e recuperação de incidentes.

19.6.2 Relato de Incidentes**:** Estabelecer um canal claro e acessível para o relato de incidentes relacionados a sistemas de IA.

19.5 Monitoramento e Melhoria Contínua

19.5.1 Monitoramento Contínuo**:** Implementar sistemas de monitoramento contínuo para detectar e responder a anomalias e ameaças aos sistemas de IA.

19.5.2 Revisão e Melhoria**:** Revisar e atualizar regularmente esta política para refletir novas ameaças, tecnologias e melhores práticas.

20. SISTEMAS TERCEIROS

20.1. Contratação de Software e Sistemas de Terceiros

20.1.1 Avaliação de Riscos: Antes de contratar qualquer software ou sistema de terceiros, é responsabilidade do contratante garantir que seja realizada uma análise completa de riscos. Isso inclui avaliar possíveis vulnerabilidades e entender como esses riscos podem impactar a segurança da nossa organização.

20.1.2 Conformidade e Requisitos Legais: O colaborador deve verificar se todos os softwares e sistemas de terceiros que utiliza foram verificados pela área de Tecnologia e estão em conformidade com as leis e regulamentações aplicáveis, como a LGPD (Lei Geral de Proteção de Dados) e o GDPR (Regulamento Geral de Proteção de Dados). Se o sistema não tiver sido verificado, é responsabilidade do colaborador que os utiliza, solicitar a análise da tecnologia para garantir a conformidade citada nesse item.

20.1.3 Due Diligence: A área de controles internos e Tecnologia são responsáveis por fazer uma análise detalhada dos fornecedores, avaliando sua reputação, práticas de segurança, histórico de incidentes e políticas de privacidade, para garantir que estamos trabalhando com parceiros confiáveis.

20.1.4 Cláusulas Contratuais: O Jurídico é responsável por incluir, nos contratos com fornecedores, cláusulas específicas sobre segurança da informação. Estas cláusulas cobrem aspectos como proteção de dados, notificações de incidentes, auditorias de segurança e responsabilidades em caso de violações.

20.2 Utilização de Software e Sistemas de Terceiros

20.2.1 É responsabilidade da área de tecnologia da Lojacorr:

a) Controlar e monitorar rigorosamente quem tem acesso aos sistemas de terceiros. Apenas o pessoal autorizado tem acesso, e sempre com os privilégios mínimos necessários para realizar suas funções;
b) Implementar um processo contínuo para garantir que todos os softwares e sistemas de terceiros sejam atualizados regularmente com os últimos patches de segurança, mantendo-nos protegidos contra novas vulnerabilidades;
c) Oferecer treinamento regular aos nossos colaboradores para que eles estejam cientes dos riscos associados ao uso de software de terceiros e saibam as melhores práticas para mitigar esses riscos;
d) Garantir que os ambientes de desenvolvimento, teste e produção para sistemas de terceiros sejam devidamente segregados. Isso minimiza o risco de acesso não autorizado e a propagação de vulnerabilidades;
e) Realizar auditorias periódicas e monitorar continuamente os sistemas de terceiros para detectar e responder rapidamente a atividades suspeitas e anomalias de segurança;
f) Garantir que todos os dados críticos armazenados em sistemas de terceiros sejam regularmente copiados e que existam planos eficazes de recuperação de desastres.

20.3. **Planos de Resposta a Incidentes**: Desenvolver e manter planos específicos de resposta a incidentes para lidar com eventos de segurança relacionados a sistemas de terceiros. Esses planos incluem procedimentos de notificação e mitigação.

20.4. **Revisão e Renegociação de Contratos:** Revisar regularmente os contratos com fornecedores de software de terceiros para garantir que continuem atendendo aos nossos requisitos de segurança da informação.

21. ACOMPANHAMENTO E REVISÃO

Esta política será revisada periodicamente para garantir que esteja sempre alinhada com as mudanças na legislação, as necessidades da Lojacorr e as melhores práticas do setor, conforme determina a POL-CI-001 - Documentos Normativos. A revisão será conduzida por Controles Internos, que apresentará os ajustes necessários à Alta Administração.

22. DISPOSIÇÕES FINAIS

Esta política é de caráter obrigatório para todos os colaboradores da Lojacorr, o seu descumprimento total ou parcial será passível de medidas disciplinares, conforme critérios previstos no Código de Conduta. Conforme determinado na POL-CI-001 - Documentos Normativos, esta Política entra em vigor na data de sua aprovação e a publicação estará disponível a todos os colaboradores e partes relacionadas a Lojacorr, na pasta do Drive e na Comunidade.

23. TERMO DE RECEBIMENTO E CIÊNCIA

Declaro ter recebido na data abaixo, lido e compreendido a "Política de Segurança da Informação" da Rede Lojacorr e assumo o compromisso de cumpri-la e respeitá-la em todas as minhas atividades na empresa, zelando por sua aplicação.

Nome completo:

Data Assinatura: