POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Versão 2

Última atualização: 11/03/2025
Classificação: Público

1 Objetivos

• Assegurar a conformidade da Política de Segurança da Informação com as normas pertinentes e legislação vigente;
• Assegurar a manutenção dos processos apoiados pelos sistemas informatizados da CATTALINI através da prevenção e solução de eventos de quebra e cumprimentos dos requisitos Segurança da Informação;
• Atender às premissas de Segurança da Informação observando os pilares: disponibilidade, confidencialidade e integridade dos nossos processos, em conformidade com os objetivos do negócio;
• Incentivar o comportamento seguro de todos os colaboradores com relação a Segurança da Informação;
• Comprometimento da Melhoria Contínua com o SGSI.

2 Definições e Siglas

Para melhor compreensão deste documento define-se a descrição dos seguintes termos ou siglas:
Risco: a possibilidade de eventos ou situações adversas que podem prejudicar objetivos, processos ou recursos de uma organização;
Disponibilidade: refere-se à informação estar disponível quando for necessária para o fim ao qual foi destinada;
Confidencialidade: refere-se à informação estar disponível e acessível somente a quem for autorizado para tal;
Integridade: refere-se à plenitude da informação, estando de acordo com as características para as quais foi desenvolvida, sem sofrer qualquer dano ou adulteração;
Autenticidade: refere-se à identidade do emissor ou receptor da informação, necessitando garantir que ambas as partes sejam quem estiver afirmando ser;
Ameaça: Causa potencial de um incidente que pode vir a prejudicar a CATTALINI, através da exploração de uma vulnerabilidade;
Ativo: Tudo aquilo que possui valor para a CATTALINI;
Endpoint: Quaisquer dispositivos móveis, incluindo, mas não se limitando a: laptops, smartphones e tablets;
Ativo de informação: Patrimônio intangível da CATTALINI, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, de natureza jurídica, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a CATTALINI por parceiros, clientes, colaboradores e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da CATTALINI ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.
Criticidade: indispensabilidade da informação para a CATTALINI.
Dados pessoais: quaisquer dados que identifiquem ou sejam identificáveis acerca da identidade de uma pessoa natural.

Dados pessoais sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (física); **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tenha possibilidade significativa de afetar as operações ou ameaçar as informações da CATTALINI.
Segurança da Informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da CATTALINI.
Sensibilidade: vulnerabilidade da informação.
Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da CATTALINI.
Contingência: Eventos imprevistos que podem ameaçar a integridade dos dados e sistemas, exigindo planos de resposta a incidentes.
Desastre: Incidente de Segurança de grande proporção com potencial de paralisar parcialmente ou completamente as operações críticas do negócio. Abrangência Esta política se aplica a todos os usuários da informação da CATTALINI, que compreende além dos colaboradores, fornecedores e prestadores de serviço que manipulam ou acessam informações em sua infraestrutura.

3 Abrangência

Esta política se aplica a todos os usuários da informação da CATTALINI, que compreende além dos colaboradores, fornecedores e prestadores de serviço que manipulam ou acessam informações em sua infraestrutura.

4 Diretrizes

A CATTALINI tem como missão a excelência dos seus serviços, segurança das suas operações, responsabilidade social e ambiental e o desenvolvimento profissional e pessoal de seus colaboradores, e desta forma assegura aos clientes qualidade e desempenho superiores, gerando sólidas relações de longo prazo.
A CATTALINI entende que a informação corporativa é um bem essencial para suas atividades e para o resguardo da qualidade e garantia dos produtos ofertados a seus clientes.
A CATTALINI compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.
Dessa forma, a CATTALINI estabelece sua Política de Segurança da Informação (PSI), como parte integrante do seu Sistema de Gestão de Segurança da Informação (SGSI), alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da organização ou sob sua responsabilidade.

O objetivo da Gestão de Segurança da Informação da CATTALINI é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à Segurança da Informação, provendo suporte às operações críticas do negócio, minimizando riscos identificados e seus eventuais impactos à organização.
A Presidência e o Comitê de Segurança da Informação e Privacidade de Dados (CSIPD) estão comprometidos com uma gestão efetiva de Segurança da Informação na CATTALINI. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

É política da CATTALINI:

a. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da CATTALINI sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
b. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: colaboradores, terceiros contratados e quando pertinente, clientes;
c. Garantir a educação e conscientização sobre as práticas adotadas pela CATTALINI de segurança da informação para colaboradores, terceiros contratados e, nas situações pertinentes, clientes;
d. Atender requisitos de segurança da informação aplicáveis ou exigidos por regulamentações e leis brasileiras e/ou cláusulas contratuais;
e. Tratar integralmente incidentes de segurança da informação, garantindo que esses sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e quando necessário, comunicando às autoridades apropriadas;
f. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
g. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.
Esta política tem por propósito preservar a Confiabilidade, Integridade e Disponibilidade das Informações, recomendando e descrevendo as condutas adequadas para o seu manuseio, controle, proteção e descarte.

5 Papéis e Responsabilidades

A Política de Segurança da Informação da CATTALINI trata sobre responsabilidades gerais da instituição, seus colaboradores, terceiros e alta Direção.
O Comitê de Segurança da Informação e Privacidade de Dados (CSIPD) desempenha um papel crucial na promoção da Segurança da Informação, atuando como um órgão de supervisão e governança, bem como, atua como um agente na promoção da cultura organizacional que valoriza a informação como um ativo crítico.

É composto por representantes de diversos departamentos da empresa, com visões isoladas - sob orientação e coordenação direta do Gestor de Segurança da Informação.

6 Sanções

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem, no caso de colaboradores, advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa, e no caso de terceiros contratados ou prestadores de serviços, a multa contratual e a rescisão do contrato.
A aplicação de sanções e punições será realizada conforme a análise do Comitê de Segurança da Informação e Privacidade de Dados (CSIPD).

7 Política de Classificação e Rotulagem de Informações

O trânsito de Informações deve ser feito por um caminho ou meio confiável com controles que ofereçam autenticidade do conteúdo, proteção de submissão e recebimento e não repúdio da origem. A operação da rotulagem das informações segue conforme **Procedimento de Classificação e Rotulagem da Informação.**

8 Acordos de Confidencialidade e Uso de Mídias

A CATTALINI reconhece a importância de manter informações confidenciais seguras, para tal seus colaboradores, contratados, parceiros de negócios e partes envolvidas comprometem-se com a Política de Segurança da Informação e o com a utilização de funcionalidades e/ou qualquer outra utilização que esteja dentro dos padrões adotados pela organização e estabelecidos em Normas e Procedimentos Gerenciais e Operacionais do Sistema de Gestão de Segurança da Informação.
Através de contrato, são estabelecidas obrigações de confidencialidade, uso de mídias e a garantia de proteção dos interesses da organização. A validade legal destes Termos somente é reconhecida pela CATTALINI e por qualquer outro órgão e/ou empresa, quando devidamente assinados pelos responsáveis legais.

9 Controles mínimos de Segurança da Informação

Os controles mínimos necessários a PSI estão listados abaixo (devem estar devidamente identificados e documentados):

- Softwares de detecção de vírus, monitoramento, filtragem Web, entre outros;
- Software de controle de acesso físico e lógico;
- Mecanismos de controle de acesso físico;
- Serviços críticos relativos à emergência (incêndio, inundações, entre outros);

• Serviços críticos relativos a concessionárias Estaduais e/ou Federais (energia, água, telefonia entre outros).

10 Monitoramento de Segurança

Testes periódicos de vulnerabilidade do ambiente de TI deverão ser realizados com a finalidade de garantir que a implementação de segurança de TI está vigiada e monitorada de forma proativa.

11 Prevenção, Detecção e Correção de Softwares Maliciosos

Medidas para prevenção, detecção e correção de Softwares Maliciosos deverão estar implementadas por toda a organização, para garantir a proteção dos ativos de informação contra softwares maliciosos. O controle dessas medidas deve estar de acordo com a **"Matriz de Riscos e SOA-Declaração de Aplicabilidade (Statement of Applicability)".**

12 Segurança em Redes

Assegurar que técnicas e procedimentos de segurança sejam usados para autorizar acessos e controlar as informações que circulam de e para as redes da organização.

13 Gestão de Capacidade

As atividades de gestão de capacidade dos recursos devem ser contínuas em todos os ambientes, conforme processo de gerenciamento **Disponibilidade e Capacidade.**

14 Política de backup

A Gestão dos Backups são realizados através do processo operacional de **Gestão de Backup Corporativo.**

15 Gerenciamento e controle de problemas

Quaisquer problemas que ocorram no ambiente operacional, sejam eles de infraestrutura, hardware, softwares e sistemas aplicativos, devem ser registrados conforme **Gestão de Problemas.**

16 Monitoramento de Segurança Física

O monitoramento de segurança física da CATTALINI é realizado por sistema de CFTV regulado por Portaria COANA.

17 Perímetro de segurança e entrada física

A CATTALINI possui controle de acesso às dependências da organização de modo a garantir a proteção de pessoas e veículos que acessam e circulam suas instalações. Tal processo é mantido pelo Departamento de Segurança Patrimonial no documento de referência externo ao SGSI denominado Norma de Acesso de Pessoas e Veículos (NAPV).

18 Política de Uso Aceitável de Informações e Ativos Associados

Estabelece as regras de comportamento desejado quanto ao uso dos ativos corporativos, bem como, detalha procedimentos que deverão ser adotados sob diversos aspectos, tais como: uso da rede, uso de e-mail, uso de acesso à internet, uso de impressoras e uso de sistemas - **Regras de Utilização de Recurso de TI.**
Somente o Departamento de TI tem autorização para realizar a instalação de quaisquer softwares ou aplicativos nos ativos da CATTALINI.

19 Política de Senhas e Identidades de Acesso

Todos os ativos ou sistemas pertencentes à CATTALINI devem ser acessados por meio de senhas. Quando o acesso for por credencial nominal (senha individual), a senha deverá ser pessoal e intransferível, sendo o seu dono o responsável por tudo que ocorrer no ambiente com o uso de suas credenciais;
Caso exista a necessidade de terceiros, tais como fornecedores ou prestadores de serviço, acessarem os sistemas e ambiente de tecnologia da CATTALINI, as credenciais de acesso de cada um deverão conter somente as permissões necessárias para a realização do trabalho ao qual foram contratados e serão fornecidas após treinamento da PSI e instruções para fornecedores na integração de terceiros.
A concessão, alteração, remoção e revisões de direitos de acesso seguem procedimento de **Gestão de Acessos e Identidades;**
Sempre que possível, os sistemas da CATTALINI deverão conter registros de logs de acesso para monitoramento e avaliação de intervenções por parte dos interessados, seguindo as práticas do **Registro de Operações e Monitoramento.**

20 Segurança de Dispositivos Endpoint

Os computadores e sistemas de comunicações não devem ser utilizados para fins pessoais.
Durante o uso de dispositivos endpoint tanto dentro quanto fora das instalações da organização, cabe ao usuário uma especial atenção à proteção do ativo.
Os softwares/aplicativos disponíveis nos dispositivos endpoint são de uso profissional e devem estar devidamente homologados e autorizados pela CATTALINI. Caso haja necessidade de utilização de um aplicativo não homologado, a solicitação deve ser feita via chamado ao Departamento de Tecnologia da Informação. Não será permitido que qualquer informação da CATTALINI seja retida exclusivamente em unidades de armazenamento local de dispositivo endpoint, devendo ser utilizados os drives de armazenamento em rede ou em nuvem disponibilizados para este fim. Os dispositivos móveis devem ser transportados de forma segura, a fim de evitar danos, furto, roubo ou extravio.

21 Política de Segurança para Trabalho Remoto

Os usuários são responsáveis por seguir as orientações contidas nesta política, bem como por tomar as medidas necessárias para proteger as informações. As diretrizes para o trabalho remoto incluem:

a) Solicitar a autorização para trabalho remoto, que deve ser aprovada pelo gestor da área e pela diretoria;
b) Utilizar apenas acesso seguro à rede, mediante VPN corporativa ativa a todo momento;
c) Não salvar senhas no navegador;
d) Usar apenas mecanismos aprovados pela organização para transferência de informações;
e) Não tentar burlar mecanismos de segurança para facilitar acessos;
f) Relatar imediatamente quaisquer suspeitas ou eventos confirmados de incidentes de segurança;
g) Manter o ativo seguro em deslocamento externo;
h) Ter cuidado ao acessar, realizar chamadas ou ceder informações em locais públicos ou com muitas pessoas como: Cafés, Shoppings, Aeroportos entre outros;
i) Manter o ativo em condições de uso.

À organização reserva-se o direito de monitorar sem aviso prévio as atividades dos usuários durante o trabalho remoto a fim de garantir a conformidade com esta política.

22 Proteção contra ameaças físicas, ambientais e contingências contra disrupções

A CATTALINI possui um Sistema de Gestão Integrado que está certificado em conformidade com as Normas ISO 14001 (Sistemas de Gestão Ambiental) e ISO 45000 (Sistemas de Gestão de Saúde e Segurança), e se adequando à ISO 27001 (Sistema de Gestão de Segurança da Informação).

Tais sistemas visam garantir a contínua avaliação de ameaças em relação à riscos físicos e ambientais, tais como incêndio, inundação, resíduos tóxicos, emissões ambientais, dentre outros que possam ocorrer nas dependências da organização em virtude das suas operações.
A CATTALINI possui redundância em suas conexões de rede, elétrica e servidores.
A ativação de tais mecanismos de proteção são expressos em um ou mais planos de resposta à desastres com testes regulares detalhados no **Gestão de Continuidade de Serviços de TI.**

23 Política de Mesa Limpa e Tela Limpa

Todos os colaboradores devem manter as mesas organizadas, com documentos confidenciais guardados em locais seguros, como gavetas e/ou armários com chaves, quando não estiverem em uso, bem como, não deve haver papéis com informações corporativas expostos.
Quaisquer impressões ou anotações contendo informações confidenciais, devem ser retiradas imediatamente da impressora.
Qualquer documento que contenha informações confidenciais deve ser destruído de forma segura quando não for mais necessário, utilizando trituradoras de papel.
É estritamente proibido anotar usuários e senhas em agendas, cadernos ou qualquer meio físico não seguro.
Os dispositivos eletrônicos, incluindo computadores, laptops e dispositivos móveis, devem ser bloqueados e protegidos por senha quando estiverem inativos ou quando o funcionário dono do ativo estiver afastado do equipamento, o bloqueio de tela será ativado por diretrizes específicas de maneira automática.
Ao usar dispositivos em áreas públicas, os colaboradores devem ter cuidado para garantir que as informações exibidas não sejam visíveis por pessoas não autorizadas, para garantir maior privacidade.

24 Camadas de Segurança

Para a devida proteção do ambiente, devem ser projetadas 4 (quatro) camadas de acesso:

- Acesso ao ambiente;
- Acesso aos sistemas aplicativos;
- Acesso às funções dos sistemas aplicativos;
- Acesso aos dados.

Sempre que possível o login e a senha de acesso devem ser únicos para todas as camadas de Segurança. Devem ser exibidos para os usuários apenas os arquivos, os softwares e as funcionalidades a que eles têm direito de acesso, ficando sob sua responsabilidade informar ao seu superior sobre acessos disponibilizados em demasia.

25 Trilhas de Auditoria

Recomenda-se a existência de softwares de Segurança e que estes mantenham registros sobre os acessos dos usuários, indicando, sempre que possível, o arquivo, o software, a data e hora que foram acessados.

As auditorias internas seguirão as definições do **Manual do SGI.**

26 Segurança da Informação para Projetos

Quaisquer projetos que visam alterar ativos, incluir novas tecnologias, alterar métodos de processamento de informação e quaisquer ações que terão impacto sobre os pilares da Segurança da Informação devem ser regidos nos termos da **Gestão de mudança de TI.**

27 Relatos de Eventos de Segurança.

Todos os membros da equipe são incentivados a relatar quaisquer eventos de segurança da informação, abrangendo incidentes, violações de dados, tentativas de acesso não autorizado ou qualquer atividade suspeita que possa comprometer a segurança dos ativos de informação no sistema de chamados da organização.
Será garantida a confidencialidade das informações fornecidas durante o processo de relato, com a subsequente implementação de medidas para investigar e mitigar os eventos de segurança, conforme apropriado e descrito no **Gestão de Incidentes.**

28 Gestão de Fornecedores

A organização realiza o gerenciamento dos seus fornecedores/terceiros para contratação de serviço. Com regras de diligência adicionais para terceiros considerados críticos à operação.
São realizadas avaliações e homologação dos fornecedores críticos através de formulário com critérios de avaliação para classificar o nível de aderência em Segurança da Informação e Privacidade de Dados.
Os fornecedores seguem as regras de acesso a informação declaradas durante a Integração de Terceiros.

29 Política de Privacidade

A CATTALINI, estabelece o tratamento de dados através da “Política de Privacidade LGPD”, disponível aos colaboradores nos canais internos da companhia, e no site para colaboradores, fornecedores, prestadores de serviços, clientes e comunidade.
Ao lidar com informações que contenham dados pessoais, sensíveis ou não sensíveis, é essencial seguir o disposto na **Política de Privacidade de Dados**. O DPO deve ser consultado em caso de dúvidas (dpo@cattaliniterminais.com.br). Isso garante que o tratamento dessas informações seja realizado de acordo com as diretrizes legais e regulamentares, mantendo a privacidade e a segurança dos dados pessoais dos indivíduos envolvidos.

30 Canal de Reporte

São disponibilizados aos colaboradores os seguintes canais para reportar incidentes de segurança, violações ou suspeitas, bem como, tirar quaisquer dúvidas acerca de temas relativos à Segurança da Informação:
a) Registro de Não Conformidade: RNC de SI
b) Portal para abertura de chamado: https://cattalini.sysaidit.com
c) E-mail para temas específicos sobre segurança da informação: ciberseguranca@cattaliniterminais.com.br
d) Ramal do Gestor de Segurança da Informação: 3508.
e) Questões inerentes à dados pessoais ou assuntos relativos à LGPD: dpo@cattaliniterminais.com.br