Título:	**Biblioteca de políticas de Segurança da Informação e Privacidade de Dados Pessoais**	Cod/Versão: BOOK-POL-001
Autor	Marcelo Silva	Data elaboração: 15/10/25
Aprovação	Ricardo Moraes	Data liberação: 11/11/25

BIBLIOTECA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS PESSOAIS

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

HISTÓRICO DAS REVISÕES

Revisão	Data	Motivo	Responsável	Ramal / E-mail
00	10/10/2025	Versão Inicial	Marcelo Silva	(11) 9 5057 3389 Marcelo.silva@w2conn.com.br
00	16/10/2025	Revisão	Marcelo Silva	

APROVAÇÕES

	Responsáveis	Áreas	Data
VALIDADO POR:	Ricardo Moraes	Corp - Administração	15/11/2025
APROVADO POR:	CEO	Diretoria	15/11/2025

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

0. SUMÁRIO

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

1. CONTEXTO DA ORGANIZAÇÃO

A empresa ENGECOMP Consultoria e Locação de Sistemas LTDA é dedicada a prestação de serviços de consultoria, assessoria e implementação de soluções relacionadas à conformidade legal empresarial, com foco em Tecnologia da Informação. Isso inclui, mas não se limita a adequação e consultoria em leis e regulamentações como a Lei Geral de Proteção de Dados (LGPD), Marco Civil da Internet, Código Civil, Consolidação das Leis do Trabalho (CLT), e outras legislações aplicáveis. Abrange também a vinculação e adoção de normas e frameworks internacionais de segurança da informação, gestão de serviços de TI e continuidade de negócios.

Processo crítico para o negócio:

- **Gerenciamento de dados corporativos com foco primário no tratamento de dados pessoais e sensíveis de titulares envolvidos em questões de privacidade e denúncias de incidentes e ilícitos.**

As orientações e decisões relacionadas a essas questões foram estabelecidas tendo em vista a autoridade do Comitê de Sócios da empresa.

1.1. PARTES INTERESSADAS

PARTE INTERESSADA: SÓCIOS / ACIONISTAS

NECESSIDADES:

a) Sustentabilidade do negócio com crescimento lucrativo em serviços de compliance, ouvidoria e privacidade (BPO, SaaS e DPOaaS).
b) Proteção do patrimônio com mitigação de riscos legais, reputacionais e operacionais.
c) Execução fiel dos aportes (tecnologia, marketing, jurídico-comercial e financeiro).

EXPECTATIVAS:

a) Posicionamento da ENGECOMP como referência em integridade corporativa, canais de denúncia e LGPD no Brasil.
b) Portfólio com receita recorrente (SaaS + BPO) e churn baixo sustentado por qualidade e conformidade.
c) Não contaminação do portfólio por incidentes de SI/PD, ética/anticorrupção ou falhas de governança.
d) Roadmap tecnológico entregue pela W2CONN conforme cronograma (Anexo I) e tração comercial/marketing conforme planos.

REQUISITOS DO SGSIPD:

a) Aderência a ISO 27001, ISO 27701, ISO 20000, ISO 22301, ISO 31000, ISO 37001 e ISO 37301 aplicáveis ao escopo.
b) Gestão de riscos integrada a canais de denúncia e privacidade, com indicadores de continuidade e auditoria interna.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

PARTE INTERESSADA: DIRETORIA (Co-CEOs e Diretores)

NECESSIDADES:

a) Governança de TI, SI e Privacidade consistente com ITIL/COBIT/NIST e LGPD, com papéis claros (Co-CEOs; CMO; CCO; Líder Jurídica).

b) Custos previsíveis e TCO otimizado em SaaS/BPO, com SLAs e métricas operacionais (SLA, MTTR, backlog).

c) Ciclo de investimento controlado com marcos de entrega do produto, compliance e marketing.

EXPECTATIVAS:

a) Segurança da Informação e Privacidade como padrão corporativo na plataforma e nos processos (by design).

b) Estado de resiliência operacional e continuidade (disponibilidade, backups, DR, planos de crise).

c) Controles financeiros e de compliance atualizados, com dashboards e auditorias periódicas.

d) Comunicação clara e tempestiva sobre eventos de segurança, incidentes LGPD e casos de denúncias sensíveis.

REQUISITOS DO SGSIPD:

a) Política integrada de Gestão de Serviços de TI, Segurança e Privacidade vigente e auditável.

b) Procedimento corporativo de resposta a incidentes de SI/PD e de crise reputacional, interoperando com a atuação da Líder Jurídica.

PARTE INTERESSADA: PRESTADORES DE SERVIÇOS

NECESSIDADES:

a) Direcionamento claro, requisitos de segurança e privacidade, e contratos com segregação de responsabilidades.

b) Remuneração e reajustes alinhados à economia, com previsibilidade de demanda (backlog) de BPO/consultoria.

EXPECTATIVAS:

a) Segurança operacional com mínimo impacto no negócio do cliente e conformidade com LGPD/código de ética.

b) Não responsabilização por eventos além de sua alçada contratual e ausência de perdas por incidentes de SI/PD.

c) Acesso a procedimentos, modelos e plataformas padronizados para garantir qualidade e rastreabilidade.

REQUISITOS DO SGSIPD:

a) Procedimentos e templates aderentes aos fluxos da ENGECOMP (ouvidoria, investigação, tratamento LGPD).

b) Due diligence e cláusulas contratuais de privacidade, confidencialidade e anticorrupção; gestão de terceiros.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

PARTE INTERESSADA: CLIENTES

NECESSIDADES:

a) Redução de risco regulatório e reputacional com operação de canal de denúncias, ouvidoria e LGPD conforme lei.

b) Melhor relação valor/preço, com SLAs claros e qualidade.

c) Entregas no prazo, tratamento diligente de denúncias e incidentes, e relatórios auditáveis.

EXPECTATIVAS:

a) Aderência estrita a contratos, LGPD, Lei Anticorrupção, normas ISO/ABNT e políticas internas do cliente.

b) Operação de serviços com níveis de qualidade e prazos acordados; transparência e rastreabilidade de casos.

REQUISITOS DO SGSIPD:

a) Transparência na comunicação de eventos/incidentes de SI/PD e reporting de status com logs/auditoria.

b) Matriz RACI clara para comunicações em crise (ANPD, autoridades, imprensa), envolvendo a Liderança Jurídica.

c) Mecanismos de consentimento, anonimato, minimização e eliminação de dados, portabilidade e registro de bases legais.

PARTE INTERESSADA: FORNECEDORES

NECESSIDADES:

a) Contratos com escopo e responsabilidades definidas, incluindo requisitos de SI, PD e ética.

b) Relação de longo prazo com previsibilidade de demanda e qualidade exigida.

c) Maximização de valor agregado nas integrações tecnológicas e serviços de suporte.

EXPECTATIVAS:

a) Clareza de responsabilidades, critérios de segurança e requisitos de integração com a plataforma.

b) Mudanças e ajustes de escopo dentro das regras contratuais e de gestão de mudanças (CAB/ITIL).

c) Não serem causadores de incidentes de SI/PD que afetem a operação da ENGECOMP ou seus clientes.

REQUISITOS DO SGSIPD:

a) Transparência sobre incidentes e crises, com SLAs de resposta e cooperação em investigações.

b) Cláusulas de privacidade, anticorrupção e segurança; avaliações periódicas de risco de terceiros (TPRM).

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

PARTE INTERESSADA: PARCEIROS DE NEGÓCIO

NECESSIDADES:

a) Diretrizes objetivas sobre papéis, responsabilidades e compliance conjunto.

b) Propostas de valor integradas (serviços e go-to-market) para ampliar alcance e market share B2B.

c) Mecanismos de co-marketing e co-selling com governança.

EXPECTATIVAS:

a) Compromisso com regras de ética, LGPD e anticorrupção, e não geração de riscos à marca ENGECOMP.

b) Operação harmônica com a plataforma e processos, respeitando confidencialidade e propriedade intelectual.

REQUISITOS DO SGSIPD:

a) Protocolos de comunicação e resposta em crise e incidentes, incluindo matriz RACI interorganizacional.

b) Due diligence de compliance e segurança para homologação de parceiros; auditoria e melhoria contínua.

1.2. PAPEL DA ENGECOMP COMO CONTROLADORA, OPERADORA E CO-CONTROLADORA NO TRATAMENTO DE DADOS PESSOAIS

1.2.1. OBJETIVO E ENQUADRAMENTO

A Empresa desempenha, de forma explícita e operacional, os papéis de Controladora, Operadora e Controladora Conjunta (Co-controladora) no tratamento de dados pessoais, em conformidade com a LGPD e com a ISO/IEC 27701.

A Empresa estabelece princípios, critérios de decisão, responsabilidades, regras contratuais e mecanismos de governança que asseguram a conformidade legal, normativa e contratual, bem como a transparência perante titulares, clientes, fornecedores, parceiros, autoridades e demais partes interessadas.

Esta declaração se apoia diretamente:

1. No contexto organizacional, nas partes interessadas e nos regulamentos aplicáveis já definidos no presente documento;
2. No Procedimento Corporativo “Relacionamento com Controladores Conjunto” (Cod/Versão: Control.V1), que estabelece critérios, responsabilidades e instrumentos para o arranjo de controladoria conjunta;
3. Na Política de Privacidade de Dados (Cod/Versão: PLP01-V1);
4. No Procedimento “Conformidade Legal e Normativa” (Cod/Versão: LEGAL.V1);
5. No Procedimento “Procedimento para Relacionamento com Fornecedores” (Cod/Versão: PRF.V1);
6. No documento “Responsabilidades do Encarregado” (Cod/Versão: DPO.V1).

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

A Empresa tem um conjunto de normas e procedimentos que definem critérios objetivos para qualificação do papel da ENGECOMP em cada contrato, campanha, plataforma e serviço correlato, garantindo a atualização do Registro de Atividades de Tratamento (RAT ou ROPA), a consistência dos avisos e bases legais, o uso proporcional de dados, e a prestação de contas (accountability) conforme ISO/IEC 27701 e LGPD.

1.2.2. PRINCÍPIOS E BASES NORMATIVAS

- **Princípios da LGPD aplicáveis:** finalidade, adequação, necessidade (minimização), livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.
- **ISO/IEC 27701:** requisitos e diretrizes para controles de privacidade aplicáveis tanto na condição de Controlador quanto de Operador, abrangendo: identificação de propósitos e bases legais (A.7.2.1-7.2.4), registros (A.7.2.8), contratos com operadores (A.7.2.6), controlador conjunto (A.7.2.7), obrigações perante titulares (A.7.3), privacy by design/default (A.7.4) e compartilhamentos e transferências (A.7.5; B.8.5).
- **Normas Internas:** Procedimentos corporativos e cláusulas contratuais padrão descritas nos documentos internos listados na seção inicial desse tópico.

1.2.3. PAPEL DA ENGECOMP COMO CONTROLADORA

Escopo principal:

- Dados de colaboradores e prestadores internos (inclusive PJs que desempenham atividades equivalentes a colaboradores): recrutamento, gestão contratual, folha, benefícios, saúde ocupacional, segurança do trabalho, gestão de acessos, registro de atividades, auditoria, prevenção a fraudes, conformidade e governança.
- Dados tratados em sistemas corporativos e nos produtos/plataformas da empresa quando a finalidade decorre da governança interna da ENGECOMP (segurança, melhoria de serviços, indicadores e métricas, continuidade de negócios e requisitos legais).

1.2.4. PAPEL DA ENGECOMP COMO OPERADORA

Escopo principal:

- Execução de contratos nos quais o cliente é o Controlador e a ENGECOMP atua sob instruções documentadas, com propósito e base legal definidos pelo cliente.

1.2.5. MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA

- Indicadores: tempo de resposta a titulares; eventos/incident response; não-conformidades e ações corretivas.
- Revisão anual desta seção ou a cada alteração material no modelo de negócios, marcos regulatórios ou contratos estratégicos.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

1.3. IMPACTO DE QUESTÕES CLIMÁTICAS NO CICLO DE SERVIÇOS DA EMPRESA E SUA INTEGRAÇÃO À CONTINUIDADE E CONFORMIDADE

1.3.1. OBJETIVO E ESCOPO

Este tópico estabelece, no contexto do presente documento, as questões climáticas e ambientais que impactam o ciclo de serviços da ENGECOMP e como os controles de continuidade (CSTI.V1) e o programa de conformidade legal e normativa (LEGAL.V1) fundamentam a preparação, a resiliência e a resposta da Empresa a eventos climáticos extremos.

O texto adapta ao nosso ambiente as diretrizes de risco operacional, continuidade de serviços, segurança física e requisitos regulatórios, assegurando que o modelo de negócios — eventos presenciais e online, ativações, incentivos e operações financeiras adjacentes — seja suportado por uma gestão efetiva de crise, comunicação, mitigação e recuperação, conforme ISO/IEC 27001, ISO/IEC 27701, práticas ITIL/COBIT e a legislação brasileira.

1.3.2. CONTEXTO, PARTES INTERESSADAS E VETORES DE RISCO CLIMÁTICO

A ENGECOMP opera com um ecossistema estrito e com ativos distribuídos entre nuvem (SaaS/IaaS/PaaS), escritórios e operação em campo (consultorias e auditorias). Eventos climáticos extremos e correlatos (enchentes, tempestades, ondas de calor, queimadas próximas, vendavais, granizo, deslizamentos, interrupções de energia e telecom, ou restrições logísticas) podem:

- Impedir ou adiar eventos presenciais;
- Impactar infraestrutura de TIC, links de comunicação, datacenters e provedores cloud;
- Aumentar incidência de incidentes correlatos (saúde de colaboradores, indisponibilidade de equipe, restrições de deslocamento).

Partes interessadas (sócios, diretoria, clientes, fornecedores, parceiros e prestadores de serviços) têm expectativas explícitas no CSTI.V1 de:

- Comunicação transparente em crise;
- RTO e MTPD adequados por tipo de serviço (24h para entregas contratuais; 8h para serviços financeiros; 48h para serviços internos TIC sem impacto direto);
- Definições claras de responsabilidades, priorização e continuidade.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

1.3.3. FUNDAMENTOS NORMATIVOS E PROGRAMÁTICOS

- Conformidade Legal e Normativa (LEGAL.V1): estabelece rotina mensal de monitoramento e implementação de mudanças legais/normativas, incluindo leis ambientais e de defesa civil que possam impor obrigações à execução de eventos e operações. Campos de workflow (impacto, áreas afetadas, prazos, responsáveis, evidências, comunicação e treinamentos) são usados para introduzir novos requisitos climáticos/regulatórios (e.g., protocolos de evacuação de locais, restrições municipais/estaduais, normas de segurança em grandes aglomerações durante eventos climáticos severos).
- Política de Continuidade de Serviços de TI (CSTI.V1): define objetivos, papéis e responsabilidades na gestão de crise, cenários de risco (inclui “Eventos climáticos extremos”), testes, comunicação de crise, integração com processos (mudanças, incidentes, disponibilidade, capacidade, configuração, segurança da informação).
- ISO/IEC 27001: controles relevantes como 7.5 (Proteção contra ameaças físicas e ambientais), 7.3/7.4 (segurança de escritórios/monitoramento físico), 5.29 (segurança da informação durante a disrupção), 5.30 (prontidão de TIC para continuidade), 5.19-5.23 (cadeia de fornecimento e nuvem).
- ISO/IEC 27701: governança de privacidade em crise (A.7.3 — obrigações com titulares; A.7.5 — compartilhamentos/transferências), com ênfase em comunicação transparente, base legal para medidas emergenciais e manutenção de direitos dos titulares.

1.3.4. CENÁRIOS CLIMÁTICOS E IMPACTOS OPERACIONAIS

Tomando por base o CSTI.V1 (6.2.2) e expandindo a lente climática:

- Enchentes urbanas: inviabilizam eventos presenciais, bloqueiam acessos logísticos; podem afetar energia em bairros/regiões, exigindo remanejamento de datas ou conversão para modelos híbridos/online.
- Tempestades e quedas de energia: afetam escritórios, hubs de operação, pontos de acesso e conectividade, tornando críticos os mecanismos de home office, links redundantes, UPS/geradores em locais do parceiro, e planos de contingência de telecom.
- Ondas de calor ou baixa qualidade do ar: exigem medidas de segurança de saúde ocupacional e adaptação de cronogramas/instalações, bem como ajustes de fornecedores de infraestrutura.
- Emergências correlatas: acionamento da defesa civil local, restrições normativas temporárias (e.g., limitação de público, interdição de áreas), que exigem rastreamento pelo programa LEGAL.V1 para pronta adequação.

Impactos potenciais no ciclo de serviços:

- Planejamento: replanejamento de ativos e cronograma; inclusão de cenários climáticos em briefings e contratos.
- Produção: checklists ambientais, inspeções e planos de evacuação; critérios de go/no-go; redundância de fornecedores críticos (estrutura, energia, telecom).
- Operação dos sistemas: escalonamento de canais digitais como fallback do presencial; robustez de infraestrutura cloud; backup e storage; monitoramento e incident response.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Backoffice (TI, SI&PD, Financeiro, Jurídico): decretação de Crise; comunicação contratual; análise de cláusulas de força maior; renegociação de entregas; compliance e registros.

Controles ISO/IEC 27001 associados:

- 7.5 Proteção contra ameaças físicas e ambientais: requisitos para locais, prevenção de danos por água, fumaça, calor; UPS/geradores (quando aplicável via parceiros); monitoramento ambiental; manutenção preventiva.
- 7.2/7.3/7.4 Segurança física: acessos, vigilância, monitoramento e coordenação com facilities/terceiros.
- 5.29/5.30 Continuidade e prontidão de TIC: inclusão de gatilhos climáticos na invocação do DR/BCP; critérios de comunicação a clientes e conformidade contratual.
- 5.19-5.23 Cadeia de fornecimento e nuvem: due diligence climática nos fornecedores críticos; cláusulas sobre resiliência, energia, telecom, sites alternativos, multirregião na nuvem; relatórios e auditorias independentes.
- 8.13 Backup e 8.24 Criptografia: proteção de dados quando ativos físicos possam ser danificados em eventos climáticos; testes de restauração e verificação de integridade.

1.3.5. PROGRAMA DE CONFORMIDADE LEGAL APLICADO A EVENTOS CLIMÁTICOS

O LEGAL.V1 determina:

- Monitoramento de requisitos legais e normativos; quando houver atos de defesa civil, decretos municipais/estaduais/federais, normas de segurança para eventos diante de fenômenos climáticos, o processo de workflow registra identificação, impacto, áreas, prazos, responsáveis, ações, evidências, comunicações e treinamentos.
- A integração com Jurídico e SIPD garante:
    - Avaliação de impacto/ajustes contratuais (força maior, remarcações, reembolsos segundo CDC quando aplicável, obrigações de segurança);
    - Atualização de políticas/procedimentos internos (checklists de campo; critérios de cancelamento seguro; comunicação a consumidores/titulares);
    - Provas de conformidade em auditorias internas/externas.

1.3.6. DADOS PESSOAIS E PRIVACIDADE EM CRISES CLIMÁTICAS

- Continuidade de proteção de dados: mesmo sob desastre, a ENGECOMP mantém padrões de segurança, confidencialidade e integridade (ISO 27701/27001). Em migrações emergenciais (p.ex., mudança de local de trabalho, uso extensivo de home-office) permanecem válidos: autenticação forte, acesso mínimo necessário, criptografia em repouso/trânsito, DLP e mascaramento quando aplicável, registros de acesso e descarte seguro.
- Obrigações perante titulares (A.7.3): garantias de acesso, correção e eliminação continuam operantes; comunicações claras de indisponibilidade temporária quando afetar o exercício de direitos; priorização de restabelecimento de canais de atendimento.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Transferências e compartilhamentos (A.7.5; B.8.5): cuidados para evitar compartilhamentos indevidos durante a crise; em co-controladoria, o ponto de contato único previamente acordado coordena comunicação e resposta.

1.4. REGULAMENTOS APLICÁVEIS

As seguintes leis e normas são os ditames legais que definem as responsabilidades do negócio:

1. LGPD, Lei Geral de Proteção de Dados Pessoais –, lei nº 13.709, de 14 de agosto de 2018;
2. Lei nº 10.406 de 10 de janeiro de 2002 (Código Civil);
3. lei nº 9.609, de 19 de fevereiro de 1998 (Propriedade intelectual de programa de computado);
4. lei nº 9.279, de 14 de maio de 1996 (Propriedade industrial);
5. lei nº 9.610, de 19 de fevereiro de 1998 (Direitos autorais);
6. Lei 12.965/2014, (Marco Civil da Internet)
7. Código Penal, art. 151, 152, 154, 154-A, 298, 307, 207, 184p3, 266.
8. Lei nº 9.296/96, art. 10 (Lei das Interceptações Telefônicas);
9. Lei 7.492/86 art 18 (violação do sigilo de operações)
10. Lei 12.846/2013 (Lei Anticorrupção)
11. Lei 8.069/90 (Estatuto da Criança e do Adolescente)
12. Lei 12.853/2013 (Lei dos direitos autorais)
13. Lei 9.605/98 (Lei de crimes ambientais)
14. Lei 8.078/90 (Código do Consumidor)
15. ABNT NBR ISO_IEC_20000
16. ABNT NBR ISO_IEC_27000
17. ABNT NBR ISO_IEC_31.000
18. Framework COBIT
19. Framework ITIL

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2. POLÍTICA SEGURANÇA DA INFORMAÇÃO CORPORATIVA

2.1. OBJETIVO

Definir as diretrizes para a implantação de práticas voltadas para a Segurança da Informação com a implementação de classificação, controles e gestão da informação, de tal forma a preservar a confidencialidade, integridade, disponibilidade e autenticidade da informação em todos os ambientes, buscando a proteção dos dados críticos, da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP, e de sua reputação no mercado, mitigando eventuais prejuízos financeiros.

2.2. APLICAÇÃO

Aplica-se a todo e qualquer usuário com acesso a qualquer tipo de informação da ENGECOMP, independente do seu vínculo com a Empresa, seja ele; gestor, colaborador, estagiário, temporário, terceiro ou de qualquer forma no âmbito de representante e/ou parceiro de negócios. Também se aplica a qualquer ativo de informação, seja servidores, sistemas, *desktops*, *notebooks*, *smartphones*, *tablets* ou a qualquer dispositivo de armazenamento, processamento ou tráfego de informações.

2.3. RESPONSABILIDADES

Sócio responsável por Tecnologia da Informação

- Proteger e gerenciar os ativos de computação disponibilizados pela ENGECOMP assegurando mecanismos para proteção adequada das informações de acordo com sua respectiva classificação;
- Disponibilizar os acessos de acordo com as diretrizes definidas pelo gestor da informação;
- Disponibilizar ferramentas para a busca e obtenção de informações.
- Apoiar os gestores das informações junto aos processos de monitoramento.

Responsável pela Operação de Tecnologia da Informação

- Coordenar as ações relacionadas à segurança da informação na ENGECOMP;
- Dar ciência periódica, aos colaboradores e prestadores de serviço, sobre a Política de Segurança da Informação Corporativa;
- Ministrar treinamentos periódicos em segurança da informação;
- Responsabilizar-se pela definição das políticas e padrões de segurança da informação da ENGECOMP;
- Apoiar os gestores das informações na definição de regras e procedimentos de concessão de acessos.
- Garantir que a segurança da informação seja parte do processo de planejamento da informação no âmbito de TI;
- Executar o controle dos acessos aos sistemas que são gerenciados pela equipe de SIT, garantindo que o processo de concessão, revogação e alteração dos acessos) seja cumprido.
- Implantar ferramentas de segurança no ambiente de infraestrutura com o objetivo de garantir a confidencialidade, disponibilidade e integridade das informações;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Elaborar procedimentos necessários para adequação dos ativos ao nível de segurança pertinentes às políticas e demais normativos da ENGECOMP;
- Tratar os incidentes de segurança da informação, no âmbito de TI;
- Apoiar e acompanhar as auditorias internas e externas de segurança da informação realizadas por clientes ou órgãos reguladores.
- Aprovar as solicitações de acessos a sistemas/informações de seus subordinados, ou prestadores de serviços sob sua responsabilidade;
- Solicitar e/ou aprovar a concessão de acessos a usuários da informação de acordo com as regras definidas pelo gestor da informação, Diretoria de Tecnologia da Informação ou outras áreas custodiantes.

Gestor ou dono da Informação (*information owner)*

- Classificar ativos da informação de acordo com a sua natureza conforme norma especificada por Segurança da Informação Corporativa;
- Estabelecer regras de proteção dos ativos de informação;
- Especificar condições para a realização de cópias de segurança;
- Aprovar novos desenvolvimentos ou manutenções que sejam de natureza evolutiva, corretiva ou novos projetos, assim como validação para sua entrada em produção;
- Apurar, com o apoio das áreas custodiantes, violações registradas e participar das ações a serem tomadas, quando da ocorrência de uma não conformidade;
- Revisar periodicamente a concessão de acessos às informações sob sua responsabilidade.

Gestor de Acesso

- Aprovar as solicitações de acessos a sistemas/informações dos empregados ou prestadores de serviços sob sua responsabilidade;
- Solicitar os cancelamentos de acessos de empregados ou prestadores de serviços que não necessitem mais do acesso no exercício de suas atribuições;
- Revisar periodicamente os acessos dos usuários da informação sob sua reponsabilidade, solicitando qualquer alteração de acessos que se faça necessária;
- Efetuar a delegação de autoridade, alçadas de aprovações para pagamentos de despesas, investimentos, movimentações financeiras e organizacionais, quando estiver ausente por motivos de férias ou licença.

Usuários da Informação

- Usar adequadamente as informações disponibilizadas;
- Manter o sigilo de suas senhas;
- Guardar de forma segura os materiais considerados estritamente confidenciais ou de uso interno;
- Comunicar a área de TI - Tecnologia da Informação de todo e qualquer desvio às normas de Segurança da Informação da ENGECOMP;
- Contribuir para a melhoria dos níveis de Segurança da Informação.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2.3.1. RESPONSABILIDADES QUANTO AOS INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Em linhas gerais, o Encarregado pelo gerenciamento dos dados pessoais é responsável por:

- Identificar a causa raiz do Incidente;
- Coordenar a resposta ao Incidente;
- Assegurar que ocorra o menor tempo de reação entre a descoberta do Incidente e o início do seu gerenciamento;
- Notificações e comunicações efetuadas sobre o Incidente;
- Medir o impacto financeiro, reputacional e operacional do Incidente, na ENGECOMP.

É responsabilidade do **comitê dos sócios no papel de Comissão de Mudanças, Privacidade e Segurança:**

- Recomendar os posicionamentos públicos e estratégicos, relativos ao Incidente;
- Alinhar o posicionamento e protocolos com a Diretoria Executiva da ENGECOMP;
- Revisar todas as notificações de comunicação do Incidente à ANPD e aos Titulares dos Dados;
- Auxiliar no posicionamento público da ENGECOMP sobre o Incidente, perante a imprensa, o mercado, colaboradores e parceiros da empresa;
- Identificar obrigações contratuais e regulatórias de reportar o Incidente para Terceiros, órgãos reguladores/governamentais (que não a ANPD), elaborar e enviar as respectivas notificações;
- Auxiliar na elaboração de estratégias de compensação aos Titulares de Dados afetados, quando tal ação for necessária;
- Recomendar a contratação de assessoria externa jurídica, quando necessário, para apoio e consultoria para a resposta ao Incidente.
- Identificar o impacto do Incidente no relacionamento com os colaboradores e processos de RH;
- Auxiliar na elaboração e divulgação das comunicações internas, quando necessárias.
- Aprovar o posicionamento da empresa sobre o Incidente, quando ele repercutir na imprensa;
- Atuar como porta-voz da empresa sobre o Incidente, quando necessário.

É responsabilidade do responsável de TI:

- Cessar a fonte de vazamento, se for o caso;
- Realizar a análise técnica do Incidente;
- Realizar a detecção, isolamento, remoção e preservação dos sistemas afetados;
- Garantir que as evidências sejam mantidas para posterior perícia técnica;
- Contratar assessoria externa para apoiar em questões técnicas, se necessário;
- Auxiliar no levantamento das informações técnicas que deverão compor as notificações e comunicados a serem emitidos pela empresa.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2.4. PRINCÍPIOS GERAIS

Os princípios estabelecidos nesta política visam permear os tópicos que apresentam relacionamento direto ou indireto com aspectos de segurança das informações, classificação, controle e gestão dessas informações utilizadas e/ou geradas na empresa em seu desempenho corporativo;

Esses princípios devem ser desdobrados em diretrizes e instruções, através de diferentes normativos visando à sua correta aplicação, execução, controle e monitoramento;

As diretrizes devem expressar estratégias, valores e o nível de comprometimento que a ENGECOMP estabelece em relação à Segurança da Informação Corporativa, bem como as respectivas instruções devem orientar o quadro de colaboradores quanto cumprimento de atividades e rotinas relacionadas ao tema;

Todos os esforços de segurança da informação devem ser projetados, implantados e mantidos buscando suportar os requisitos de negócio da ENGECOMP, observando práticas de análise de risco e procurando um alinhamento a esta política;

Situações específicas não contempladas ou que estejam conflitantes com esta política devem ser analisadas pela equipe de TI, formalizadas através de documento próprio e apresentadas às Diretorias Executivas para a aprovação e continuidade do processo. As áreas de Controles Internos e de Auditoria Interna poderão ser envolvidas sempre que se fizer necessário;

A revisão desta política e dos normativos derivados deve ser realizada de forma periódica para que esses instrumentos estejam permanentemente atualizados;

A ENGECOMP reserva-se o direito de, a qualquer momento e sem aviso prévio, monitorar, auditar ou fazer cópias de segurança de qualquer dado e/ou informação armazenado(s) em ativos de sua propriedade.

2.5. ATIVOS DE INFORMAÇÃO

Os ativos de informação vinculados à Empresa pertencem a ENGECOMP, não importando seu meio físico ou lógico de armazenamento. Seu uso se dará apenas e tão somente dentro do escopo das atividades de negócio da ENGECOMP;

Controles tecnológicos e/ou processuais serão utilizados com o objetivo de proteger e minimizar os riscos associados ao uso das informações ou ativos de processamento de modo a preservar suas características de segurança;

A gestão de ativos da informação deve especificar, sempre que possível, requisitos para inventariar e identificar o responsável dos ativos de informação, independente do seu meio de acesso, mantendo a proteção adequada de acordo com a proteção ideal;

A informação produzida ou transformada por qualquer processo da ENGECOMP é considerada como um ativo da Empresa. Desta forma, os ativos de informação da ENGECOMP, assim como os seus respectivos ativos de processamento, devem ser identificados, controlados e armazenados adequadamente de forma a proteger seus requisitos de integridade, confidencialidade, legalidade e disponibilidade;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Todas as pessoas físicas ou jurídicas que prestam serviços internos ou externos devem utilizar os ativos de acordo com as cláusulas contratuais firmadas com fornecedores, parceiros e clientes. A utilização de ativos da informação deve respeitar a legislação vigente e as normas internas da ENGECOMP.

2.6. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Todos os assuntos que tenham relacionamento com a TI - Tecnologia da Informação da ENGECOMP deverão ser analisados e tratados dentro da esfera adequada, seguindo os princípios e definições desta política;

Para a aplicação e o acompanhamento e dos tópicos relativos à Segurança da Informação Corporativa, fica estabelecida o endereçamento ao **comitê dos sócios no papel de Comissão de Mudanças, Privacidade e Segurança:**

Devem ser estabelecidos canais de comunicação específicos, possibilitando os meios necessários à realização de denúncias de não aderência aos princípios desta política ou outras situações que ponham em risco a segurança das informações da ENGECOMP.

2.7. CLASSIFICAÇÃO DOS ATIVOS DA INFORMAÇÃO

Os ativos de informação deverão ser classificados de acordo com seu nível de confidencialidade, disponibilidade, integridade e características legais de controle, de forma a serem adequadamente protegidos, acessados, armazenados, tratados, transportados e descartados, conforme apresentado abaixo:

- **ESTRITAMENTE CONFIDENCIAL:** Esta categoria se aplica à informação que deve ser utilizada somente dentro do âmbito da ENGECOMP, restrita a um grupo limitado de componentes. Sua divulgação não autorizada pode impactar muito seriamente a ENGECOMP e seus clientes;
- **USO INTERNO:** Esta categoria se aplica à informação que se destina ao uso dentro do âmbito da ENGECOMP;
- **PÚBLICA:** Esta categoria se aplica à informação que pode ser divulgada e acessada pelo público em geral e para a qual sua divulgação e conhecimento generalizado não causam nenhum conflito ou dano, nem a ENGECOMP e nem a terceiros.

Todos os ativos de informações, quando não estiverem devidamente classificados, identificados ou divulgados devem ser considerados de uso interno.

2.8. SEGURANÇA FÍSICA E DO AMBIENTE

Os ativos de informação devem ser protegidos contra danos (acidentais ou intencionais), roubo e/ou interrupções ou quaisquer eventos que gerem sua indisponibilidade;

Deve ser estabelecido um perímetro mínimo de segurança física de forma a preservar o acesso somente a pessoas devidamente autorizadas para tal, conforme previsto normativo sobre o tema;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

A prática de mesa limpa deverá ser adotada, de forma a promover a segurança dos ativos de informação, classificados como estritamente confidenciais; bem como o processamento e a guarda de dados críticos devem ser efetuados em áreas com segurança apropriada.

2.9. SEGURANÇA DE RECURSOS HUMANOS

O processo de recrutamento e seleção de candidatos, cujos critérios estão descritos em normativo específico, deve apresentar aos aprovados os princípios da ENGECOMP e de conduta relacionados nas Políticas de Governança Corporativa e Código de Ética;

Toda quebra das regras de confidencialidade pelo quadro de colaboradores, bem como qualquer ação que venha a violar os termos desta política deverá ser tratada pelo Comitê de Ética;

Os acordos de confidencialidade de informações devem ser incluídos nos termos dos contratos de trabalho ou prestação de serviço, os quais devem ser assinados pelos envolvidos ou seus responsáveis legais. As responsabilidades dos colaboradores devem ser estabelecidas no que concerne à segurança dos ativos de informação sob sua tutela;

Todo colaborador da ENGECOMP, quando for desligado, deverá entregar os recursos que lhe foram disponibilizados pela empresa *(notebooks*, *smartphones*, etc.);

A utilização de terceirizados e/ou prestadores de serviços em processos nos quais informações “estritamente confidenciais” ou “internas” sejam trabalhadas, devem ser particularmente controladas através dos meios cabíveis (contratos e processos de monitoração), de forma a contemplar os requisitos de segurança da informação estabelecidos pela ENGECOMP;

Todo novo parceiro contratado pela ENGECOMP deve atender aos requisitos de TI - Tecnologia da Informação previstos em normativo específico sobre o tema.

2.10. TRATAMENTO DE FRAUDE

Controles específicos que visem à redução das possibilidades de fraude devem ser implementados de forma sistêmica, tais como:

- Validação periódica dos acessos quanto à sua necessidade e aderência funcional;
- Segregação de funções entre os usuários;
- Funcionalidades relacionadas a rastreabilidade das ações nos sistemas.

Todas as ocorrências de fraudes devem ser investigadas, registradas e tratadas de forma condizente com a dimensão da situação pelas áreas responsáveis pela sua prevenção.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2.11. UTILIZAÇÃO DE CORREIO ELETRÔNICO, TELEFONIA E INTERNET

Os serviços de acesso à internet, correio eletrônico e telefonia fixa também são ativos da ENGECOMP disponibilizados para a realização das atividades durante a jornada de trabalho; desta forma, os usuários não devem utilizar os recursos para fins não condizentes com suas funções e responsabilidades profissionais;

O acesso à ferramenta de Webmail da ENGECOMP somente deve ser liberado mediante aprovação da área responsável, tendo em vista que este tipo de acesso é restrito a um grupo específico de pessoas;

Esses serviços corporativos não são privativos. Controles de monitoramento e acompanhamento dos serviços acessados pelos usuários devem ser estabelecidos, visando ao bloqueio do acesso a sites de Internet, bate-papo e facilidades de telefonia não relacionados às necessidades corporativas da ENGECOMP;

Os colaboradores da ENGECOMP estão proibidos de utilizar a internet de maneira que viole os acordos de privacidade de outros usuários ou infrinja legislações vigentes (leis de direitos autorais, calúnia e difamação, etc.);

Mecanismos específicos de criptografia devem ser adotados para a transmissão de informações classificadas como “estritamente confidencial”, via internet, independente do meio de comunicação ou da mídia utilizada para tal.

2.12. CONFORMIDADE E GESTÃO DE SOFTWARE

Somente devem ser utilizados *softwares* que já estejam previamente homologados pela área de TI, não sendo tolerada a utilização de *softwares* sem licença ou cópia não autorizadas, sem permissão formal da área de TI;

Toda mudança de utilização de *software* deve ser previamente avaliada e aprovada pelas áreas envolvidas em conjunto com TI, considerando-se os impactos no ambiente computacional da ENGECOMP;

Uma estrutura específica de controles internos de TI deve ser estabelecida, de forma que garanta a segurança dos sistemas que suportam o atendimento aos aspectos legais;

Deve-se estabelecer uma avaliação interna (auditoria interna) e outra avaliação independente (auditoria externa) sobre a estrutura de controles de Segurança de TI visando identificar, verificar, validar e emitir um parecer sobre sua efetividade operacional.

2.13. GESTÃO DE DISPOSITIVOS DE SEGURANÇA DE TI

A gestão de dispositivos de segurança vinculados a TI deve ser tratada única e exclusivamente pelas áreas responsáveis de TI, de forma a promover a melhor solução para cada situação;

Todos os computadores (*desktops*, *notebooks*, *laptops*, servidores, etc.) instalados na ENGECOMP devem ser monitorados constantemente para a eliminação de vulnerabilidades de segurança identificadas e a aplicação de correções de segurança reportadas pelos fabricantes (*patches*);

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Todos os recursos computacionais da ENGECOMP devem estar providos de *softwares* antivírus, bem como os processos estabelecidos que garantam a atualização das vacinas;

Notebooks, laptops e dispositivos semelhantes de colaboradores que possuem cargos elegíveis para tal devem possuir mecanismos de segurança implantados, tais como criptografia no armazenamento de dados e mecanismos específicos;

Mecanismos específicos de controle de *e-mails* indesejados (*spam*, etc.) devem ser adotados e implementados, bem como aqueles destinados à detecção de intrusos em comunicações da rede interna corporativa com o meio externo e ainda quaisquer outras soluções protetivas que se façam necessárias.

Aplicação de Hardening / Padrões de Configuração: Cabe à equipe de TI - Tecnologia da Informação desenvolver e monitorar os padrões de segurança, bem como a responsabilidade em aplicar padrões de configuração para todos os componentes dos sistemas.

Segurança na Arquitetura das Aplicações: A ENGECOMP deve fazer uso das boas práticas de arquitetura das aplicações e a segregação em camadas de apresentação, aplicação, banco de dados com o objetivo de proporcionar a padronização de desenvolvimento e implantação de soluções;

Certificados Digitais: Toda aplicação que contenha informações da ENGECOMP e esteja hospedada em ambiente externo devem suportar comunicação com protocolo seguro. Todo e qualquer certificado digital em uso na ENGECOMP para aplicação interna classificada como crítica deve ser emitido utilizando a autoridade certificadora homologada pela área de TI da ENGECOMP.

Exceções ou desvios devem ser formalizados em documento próprio que contemple uma análise de riscos e controles compensatórios quando necessário e apresentados ao **comitê dos sócios no papel de Comissão de Mudanças, Privacidade e Segurança:** em conjunto com a Diretoria Executiva demandante para deliberação.

2.14. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Devem ser estabelecidas sistemáticas que venham a promover um controle satisfatório de todas as alterações e mudanças realizadas, de tal forma que os programas que estejam em produção sejam submetidos a um controle específico, identificando e registrando as modificações significativas, avaliando o impacto potencial das mudanças, obtendo as aprovações pertinentes e comunicação às partes interessadas;

De forma a reduzir o risco de mau uso, acidental ou deliberado dos sistemas, deve-se aplicar uma adequada segregação de funções entre os administradores do ambiente de produção e os desenvolvedores de sistemas;

Todas as alterações ou desenvolvimentos nos ambientes dos sistemas devem ser realizados conforme metodologias utilizadas pela Diretoria de TI, sendo padronizadas, registradas, aprovadas, testadas e documentadas, conforme normativo específico;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

Para proteger as aplicações *web* da ENGECOMP e para mitigar os riscos de apropriação das vulnerabilidades, devem ser adotadas as boas práticas de desenvolvimento seguro como, por exemplo, OWASP.

2.15. CONTINUIDADE DO NEGÓCIO (BACKUP E PLANOS DE CONTINGÊNCIA)

De forma a promover a continuidade do negócio, evitando sua interrupção e a proteção dos processos críticos contra falhas ou desastres significativos devem ser estabelecidas sistemáticas que promovam a restauração dos sistemas em casos de perdas;

Cabe ao *information owner* determinar quais são os ambientes críticos e, com o apoio da área de TI - Tecnologia da Informação e da Diretoria de Tecnologia da Informação, coordenar a elaboração, atualização e testes periódicos de Plano de Continuidade para os recursos computacionais de TI;

Devem ser estabelecidas formas e rotinas de *backups* que zelem por todas as informações corporativas armazenadas em meio magnético, utilizando as práticas mais adequadas disponíveis;

Todos os sistemas vigentes que gerem dados e informações críticas devem passar por rotinas de *backups* periódicos, de forma a garantir a manutenção da informação em caso de perda, dano ou roubo;

Sempre que ocorrerem mudanças consideradas significativas em sistemas operacionais e/ou *upgrades* devem ser executadas rotinas de *backup*;

As mídias derivadas dos *backups* devem ser armazenadas isoladamente, com acesso restrito às pessoas autorizadas e devidamente protegidas contrafogo, alagamento e semelhantes;

Todos os planos de contingência desenvolvidos deverão passar por testes, verificando sua funcionalidade e correção de eventuais desvios, devendo estar devidamente registrados e documentados.

2.16. CONTROLE DE ACESSO LÓGICO DOS USUÁRIOS

Cada colaborador, prestador de serviços ou fornecedor deve possuir, uma única conta (*username /login*) pessoal e intransferível, conforme o perfil de acesso definido, devendo os usuários ser identificados e registrados nos acessos aos recursos de informática;

O fornecimento de uma conta (*username/login*) para terceiros somente será cedido em casos específicos mediante aprovações;

Para elevar o nível de segurança dos acessos, os usuários devem definir para si senhas fortes como meio de validação de sua identidade quando dos acessos a estações de trabalho, redes, sistemas, servidores, etc., tal como recomendado pelas boas práticas de Segurança da Informação;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Toda concessão de acesso aos sistemas de TI deve ser efetuada de acordo com as necessidades de negócio, devendo ser previamente aprovada pelo gestor responsável; em observância às regras estabelecidas para a gestão do sistema em questão;

O período de duração da concessão do acesso deve ser pertinente à função do usuário e de acordo com as orientações do *information owner*, devendo ser cancelada ao fim do contrato de prestadores de serviço e terceiros ou do desligamento do colaborador da ENGECOMP;

Toda vez que uma conta de usuário (*username/login)* for cancelada, não deverá ser reutilizada, devendo os acessos a todos os sistemas vinculados à conta ser excluídos ou bloqueados; exceto para o Segmento Pessoal. No Segmento Pessoal, quando um usuário (colaborador) for desligado e contratado novamente, ele receberá o mesmo *login* utilizado no passado (este cenário é específico para colaboradores);

Periodicamente, as contas dos usuários e seus privilégios nos aplicativos devem ser verificados ou atestados, de forma a promover a manutenção e atualização da base de cadastro, exclusão de usuários desligados, contas em desuso ou em duplicidade;

Todo acesso aos sistemas aplicativos deve promover a sua correta autenticação utilizando-se seu *username/login* e senha, de forma a permitir a identificação individualizada do usuário preservando a rastreabilidade das ações;

Todos os sistemas que a área de Controles Internos definir como críticos para o negócio devem ser identificados e possuir trilhas de auditoria habilitadas, devendo ser registradas todas as operações privilegiadas, início e finalização do sistema, conexão e desconexão de dispositivos, tentativas de acesso não autorizadas, violação de *gateways* e *firewalls*, dentre outros.

2.17. SEGURANÇA EM MANUSEIO DE MÍDIAS

A utilização de mídias removíveis que permitem gravação, tais como: *pendrive* e gravador de CD ou DVD deve ser limitada a diretores, gerentes e gerências jurídicas (para colaboradores autorizados) e de Segurança da Informação; demais colaboradores devem justificar a necessidade de uso para serem aprovadas pela subcomissão de Segurança e Privacidade.

2.18. BYOD – USO DE EQUIPAMENTOS E DISPOSITIVOS PESSOAIS

A utilização de equipamentos pessoais conectados à rede corporativa da ENGECOMP e suas Unidades de Negócio (Empresarial, Pessoal e Residencial & Combos), é permitido apenas em casos aprovados pelas diretorias Executivas da ENGECOMP;

O acesso remoto de colaboradores autorizados em virtude de atividades de suporte e cargos de confiança somente deverá ser efetuado através dos recursos liberados pela área de Infraestrutura de TI, onde existem controles de segurança implantados que podem garantir a confidencialidade e integridade das informações.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2.19. CLOUD COMPUTING

Toda a empresa contratada para a prestação do serviço de *cloud computing* deve disponibilizar a modalidade *Private Cloud* (Nuvem Privada), a fim de que possa assegurar a administração de itens como gerenciamento de redes, configurações do provedor, tecnologias de autenticação e autorização e criptografia dos dados transmitidos e armazenados possa ser realizada e/ou definida pela ENGECOMP em normativo específico.

Deve haver no contrato itens que;

- Visem garantir a integridade, confidencialidade, disponibilidade, autenticidade e não-repúdio das informações manipuladas;
- Plano de Contingência dos dados (incluindo recuperação de dados e administração de incidentes);
- ANS (Acordos de Nível de Serviço) e ANO (Acordo de Nível Operacional);
- Modelo de Gestão de Riscos;
- Garantir a gestão dos acessos conforme política de gestão de acesso lógico;
- Dever haver registro dos *logs* de acessos e *logs* de transações do sistema.

A empresa contratada deve garantir a segregação dos dados da contratante e oferecer total apoio em casos de investigação solicitado pela contratante, com prazos de retorno definidos em ANS.

2.20. TRATAMENTO DE INCIDENTES

Todos os incidentes de segurança física e/ou lógica, ocorridos no âmbito da ENGECOMP e suas Unidades de Negócios ou empresas prestadoras de serviço que estejam envolvidas no processamento de dados devem ser imediatamente comunicados às áreas responsáveis, não sendo permitido qualquer tipo de investigação por outras áreas;

A equipe de TI detém autonomia para tomar decisões operacionais relacionadas aos incidentes de segurança, devendo requisitar a participação de qualquer colaborador ou fornecedor para auxiliar na análise e/ou resolução do incidente;

Todos os incidentes de segurança deverão ser classificados conforme grau de magnitude. Para casos extremos, deverá ser envolvida a Subcomissão de Segurança e Privacidade para gerir e registrar toda a situação, conforme normativo específico sobre o tema.

2.21. TRATAMENTO DE INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Esta instrução tem como objetivo estabelecer as normas procedimentais em caso de Incidentes de segurança de Dados Pessoais. Com essa informação os Colaboradores estarão preparados para:

- Classificar os Dados envolvidos;
- Classificar a criticidade do Incidente;
- Minimizar eventuais danos gerados para os Titulares dos Dados Pessoais;
- Minimizar eventuais danos gerados para a ENGECOMP.

Em caso de Incidentes, a resposta adequada será fundamental para a minimização dos danos causados aos Titulares dos Dados afetados e à ENGECOMP.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

As atividades relacionadas a estes incidentes seguem abaixo:

a) Reportar possíveis Incidentes de violação de Dados pessoais prontamente.

b) O colaborador que notar um incidente desse tipo deve tomar nota dos eventos que o levaram a creditar que um Incidente esteja ocorrendo (data, hora, sistemas, computador ou pessoas afetadas/envolvidas);

c) O Encarregado será o responsável por monitorar estes alertas por parte de colaboradores e terceiros e fazer a análise inicial dos reportes recebidos, de forma imediata, juntamente com o gestor da área de Segurança da Informação.

d) A área de Segurança da Informação deverá conduzir, periodicamente, o monitoramento preventivo de sistemas, uso de web e mensagens de correio eletrônico, conforme descrito na Política de Segurança da Informação.

e) Caso o reporte inicial não contenha informações suficientes para a avaliação da ocorrência do Incidente, o Encarregado ou o gestor da área de Segurança da Informação solicitará informações complementares ao informante.

f) Não havendo a existência de indícios razoáveis de que o Incidente ocorreu, o reporte deverá ser formalizado em relatório e arquivado, indicando, ainda, as razões do arquivamento.

2.21.1. CLASSIFICAÇÃO DO INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS

Constatada a ocorrência de um Incidente, o Encarregado classificará o Incidente conforme a seu impacto no titular ou na ENGECOMP e o tipo de dado envolvido.

Quanto ao tipo de dado, pode-se considerar a seguinte classificação:

- **Genérico:** Quaisquer informações relativas a uma pessoa singular identificada ou identificável, e que não esteja classificada abaixo como Dados Financeiros e/ou Comportamentais.
- **Financeiro:** Dados pessoais que que remetam ou revelem qualquer aspecto da vida financeira do Titular. Exemplos: número de conta, cartão de crédito, código verificador, renda, salário, benefícios.
- **Comportamental:** Dados pessoais que demonstrem ou revelem o comportamento do Titular. Exemplos: Dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.
- **Sensível:** Dados Pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, Dado genético ou biométrico, quando vinculados a uma pessoa natural.

Considerando o impacto nas partes envolvidas, seja no Titular ou na ENGECOMP, é responsabilidade do Encarregado a notificação do Incidente para a ANPD e para os Titulares, quando cabível.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2.22. VIOLAÇÃO DOS TERMOS DESSA POLÍTICA

Violações a esta política estão sujeitas às sanções disciplinares, observadas a natureza e a gravidade da infração, sendo passíveis de punições, e em conformidade com a legislação trabalhista, sem prejuízo de outras sanções penais e civis;

São consideradas também violações a esta política as seguintes situações:

- Não cumprimento das diretrizes e requisitos estabelecidos nas políticas de Segurança Corporativa da ENGECOMP;
- Uso indevido e divulgação não autorizada de informações, segredos comerciais ou outras informações sem autorização formal do gestor da informação e da área de TI - Tecnologia da Informação (para garantir a forma correta de divulgação ou de disponibilização);
- Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis, regulamentos internos e externos e Código de Ética Corporativa da ENGECOMP;
- Qualquer situação que exponha a ENGECOMP a perdas financeiras ou comprometimentos de imagem, em decorrência da quebra da confidencialidade, integridade ou disponibilidade das suas informações ou das quais que detenham custódia.

2.23. REFERÊNCIAS

- **POLÍTICAS DE GOVERNANÇA CORPORATIVA E CÓDIGO DE ÉTICA**;
- **ABNT NBR ISO/IEC 27001:2013:** Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;
- **ABNT NBR ISO/IEC 27002:2005 –** Tecnologia da Informação: Técnicas de Segurança – Diretrizes para Implantação de Um Sistema de Gestão da Segurança da Informação;
- **ABNT NBR ISO/IEC 27011:2005 –** Tecnologia da Informação: Técnicas de Segurança - Gestão da Segurança da Informação em Organizações de Telecomunicações.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

3. POLÍTICA DE USO ACEITÁVEL DE RECURSOS DE TI

3.1. OBJETIVO

Estabelecer a sistemática para a gestão do uso aceitável dos recursos de Tecnologia da Informação e gerenciamento do ciclo de vida de ativos e serviços junto a ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

3.2. DIRETRIZES GERAIS PARA O USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

As principais diretrizes para esta política são:

a) As informações são armazenadas e veiculadas por diferentes formas, incluindo os recursos de tecnologia da informação, e são essenciais ao desempenho das atribuições da Empresa;
b) As normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO IEC 27001:2022 e 27002:2022 que estabelecem, respectivamente, o sistema de gestão e o código de boas práticas em segurança da informação recomendam o estabelecimento de regras para o uso aceitável dos ativos de tecnologia da informação;
c) O preconizado no documento COBIT® 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES que define um modelo de gestão e código de boas práticas para controle e governança de ativos de tecnologia da informação;
d) A LGPD, Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais;
e) A Lei Federal nº 9609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador;
f) O Estatuto da Criança e do Adolescente (ECA), Lei Federal nº 8.069, de 13 de julho de 1990, que regulamenta o artigo 227 da Constituição Federal e define as crianças e os adolescentes como sujeitos de direitos, em condição peculiar de desenvolvimento, que demandam proteção integral e prioritária por parte da família, sociedade e do Estado;
g) A Lei Carolina Dieckmann, lei Nº 12.737/2012 voltada para crimes virtuais e delitos informáticos;
h) A Empresa se reserva no direito de inspecionar, sem a necessidade de aviso prévio, os computadores e qualquer arquivo armazenado, estejam no OneDrive Corporativo, disco local dos computadores, nas áreas privativas ou nas áreas compartilhadas da rede, visando assegurar o rígido cumprimento desta política.

3.3. ATIVIDADES PERMITIDAS E DIREITOS DOS USUÁRIOS INTERNOS

O uso dos recursos de Tecnologia da Informação pelos usuários internos e externos, destina-se às atividades relacionadas com suas atribuições funcionais.

Os recursos de Tecnologia da Informação devem ser utilizados respeitando-se os direitos de propriedade intelectual de qualquer pessoa ou empresa.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Respeitado o disposto na Lei Federal nº 9609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade da Empresa os programas desenvolvidos para a empresa por usuários internos e externos.

São garantidos aos usuários internos, no exercício de suas funções, após aprovação em treinamento específico:

a) Ter conta para acesso à rede corporativa;
b) Fazer uso legal dos recursos de TI colocados à sua disposição, respeitadas as normas de utilização estabelecidas pela Empresa;
c) Ter acesso às informações que lhe são franqueadas nas áreas privativa e compartilhadas com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança;
d) Ter acesso remoto à rede corporativa, utilizando recursos próprios, observados os requisitos de segurança estabelecidos pela área de tecnologia da Empresa;
e) Solicitar suporte técnico à área de tecnologia.

Sempre que for necessário para atividades de administração dos recursos de tecnologia e suporte técnico ou nos casos de suspeita de violação de regras, a área de segurança da informação poderá acessar arquivos de dados privativos ou compartilhados.

3.4. ATIVIDADES PERMITIDAS E DIREITOS DOS USUÁRIOS EXTERNOS

O uso dos recursos de TI pelos usuários externos, destina-se às atividades relacionadas com suas atribuições estabelecidas em contrato.

Os recursos de TI deverão ser utilizados respeitando-se os direitos de propriedade intelectual de qualquer pessoa ou empresa.

Respeitado o disposto na Lei Federal nº 9609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade da Empresa os programas desenvolvidos para a empresa por usuários internos e externos.

Considerando os limites estabelecidos em contrato com a empresa responsável pelo usuário externo, são garantidos aos mesmos no exercício de suas funções, após aprovação em treinamento específico:

a) Ter conta para acesso à rede corporativa;
b) Fazer uso legal dos recursos de TI colocados à sua disposição, respeitadas as normas de utilização estabelecidas pela Empresa;
c) Ter acesso às informações que lhe são franqueadas nas áreas privativa e compartilhadas com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança;
d) Ter acesso remoto à rede corporativa, utilizando recursos de tecnologia próprios, observados os requisitos de segurança estabelecidos pela área de tecnologia da informação;
e) Solicitar suporte técnico à área de tecnologia da informação.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Sempre que for necessário para atividades de administração dos recursos de tecnologia e suporte técnico ou nos casos de suspeita de violação de regras, a área de tecnologia da informação poderá acessar arquivos de dados privativos ou compartilhados.

Nos contratos e convênios celebrados com a Empresa, os contratados e os conveniados deverão anuir formalmente à Política de Segurança da Informação e à Política de Uso Aceitável dos Recursos de Tecnologia da Informação por meio de instrumento adequado, seja via contrato ou aditivo, assim como comprovar que os seus usuários e prestadores de serviços, também assumiram tal compromisso.

3.5. ATIVIDADES VEDADAS AOS USUÁRIOS INTERNOS E EXTERNOS

É vedado o uso dos recursos de tecnologia da Empresa para processar, guardar ou encaminhar material de cunho político, não ético, discriminatório, malicioso, obsceno ou ilegal, além de atividades visando:

a) Promoção pessoal;
b) Venda de produtos ou engajamento em atividades comerciais de qualquer natureza;
c) Constrangimento, assédio, calúnia, injúria, difamação, ameaça, ofensa ou agressão;
d) Distribuição voluntária de mensagens não desejadas, como circulares, manifestos políticos, correntes de cartas ou outros sistemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os recursos de TI;
e) Ocultação de sua identidade quando utilizar os recursos de TI;
f) Acesso não autorizado ou indevido aos recursos de TI;
g) Violação dos sistemas de segurança dos recursos de TI, no que tange à identificação de usuários, senhas de acesso, sistemas de alarme, registro de eventos (log) e demais mecanismos de segurança e restrição de acesso;
h) Instalação, alteração ou remoção de software sem acompanhamento ou autorização da equipe técnica da área de TI.

3.6. OBRIGAÇÕES DOS USUÁRIOS INTERNOS E EXTERNOS

São obrigações de todos os usuários internos:

a) Manter em caráter confidencial e intransferível códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.);
b) Alterar periodicamente a senha de acesso de acordo com os procedimentos estabelecidos pela área de TI;
c) Zelar por toda e qualquer informação disponível pelos recursos de TI da Empresa contra alteração, destruição, divulgação, cópia e acesso não autorizados;
d) Desligar ou bloquear computadores em uso quando houver necessidade de ausentar-se fisicamente do local;
e) Fazer manutenção na sua área privativa periodicamente, evitando o acúmulo de informações desnecessárias.
f) Manusear dados pessoais e sensíveis dos Titulares de clientes conforme as regras de transferência entre cliente e Empresa definidas pela área de TI.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

g) O pessoal interno da Empresa deve firmar compromisso com as práticas, responsabilidades e obrigações normativas referentes à Política de Segurança da Informação e à Política de Uso Aceitável dos Recursos de Tecnologia da Informação.

3.7. OBRIGAÇÕES DA DIRETORIA RESPONSÁVEL PELAS ÁREAS DE TI, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

São obrigações da área de TI:

a) Manter e monitorar o uso dos recursos de tecnologia disponibilizados sem interrupções, exceto em casos de imprevistos ou manutenção técnica programada;
b) Monitorar a observância deste normativo, devendo, em caso de descumprimento, tomar medidas imediatas de restrições de uso dos recursos, de acordo com o disposto nas normas da empresa;
c) Implantar autorização ou restrição de acesso às informações, disponíveis através dos recursos de tecnologia;
d) Cancelar o acesso aos recursos de tecnologia disponíveis imediatamente após o término do vínculo do usuário interno ou colaborador;
e) Gerenciar os privilégios de usuários, as senhas de usuários, os procedimentos de logon e de regras de troca de senha;
f) Desenvolver, adquirir, manter e auditar os sistemas de informação;
g) Registrar as ações dos usuários internos na rede corporativa, inclusive o histórico de utilização da internet;
h) Proteger e manter a segurança dos dados armazenados na rede corporativa;
i) Realizar a cópia de segurança de dados armazenados em discos de servidores da rede local;
j) Manter atualizadas as configurações necessárias para o acesso externo à rede corporativa, e orientar os usuários internos e colaboradores sobre seu uso e requisitos de segurança;
k) Orientar sobre a configuração dos recursos de tecnologia;
l) Providenciar o controle da adesão dos usuários internos as práticas, responsabilidades e obrigações previstas na Política de Segurança da Informação e seus normativos correlatos;
m) Administração da área de Segurança da Informação e Privacidade de Dados.

3.8. UTILIZAÇÃO DOS RECURSOS DE TI

Todos os procedimentos de manutenção, instalação, desinstalação, configuração e alteração de hardware e software em recursos de TI disponibilizados pela Empresa são prerrogativa exclusiva da área de Tecnologia da Informação.

Compete à essa área definir os recursos, bem como homologar a utilização de hardware ou software de propriedade do usuário no ambiente computacional da Empresa.

Aos técnicos da equipe de suporte de TI são dados o direito de acesso remoto aos computadores e dispositivos móveis da Empresa, em utilização pelos usuários, para fins de manutenção. O acesso remoto para suporte na área privativa do usuário apenas será iniciado mediante sua anuência, que deve acompanhar todas as operações executadas pela equipe técnica.

As configurações e atribuições de parâmetros em todos os recursos conectados à rede estar de acordo com as políticas e normas internas de gerenciamento.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

As atividades dos usuários poderão ser reconstituídas a partir de registros de atividades (logs).

3.9. SOBRE O CONTROLE DE ACESSO A SISTEMAS E APLICAÇÕES

O controle de acesso é um dos mecanismos utilizados para proteger o ambiente de tecnologia. O acesso aos recursos de tecnologia deve ser permitido somente a entidades autorizadas, como usuários internos e externos, de acordo com a Política de Segurança da Informação.

O direito de uso de qualquer recurso de TI cessa quando o usuário terminar o seu vínculo com a Empresa.

O colaborador que permanecer em licença com duração superior a 180 (cento e oitenta) dias terá direito de acesso aos recursos de TI revisado conforme o regramento interno aplicado ao caso.

O colaborador que tiver sua relação contratual com a Empresa encerrada terá seu acesso aos recursos de TI suspenso. Dados pessoais mantidos em sistemas de armazenamento corporativo deverão ser auditados antes de liberados para no distrato. Contas de acesso serão direcionadas para o gestor da área. Após 60 (sessenta) dias do desligamento, as contas serão apagadas ou anonimizadas.

O prestador de serviços interno que tiver sua relação contratual com a Empresa encerrada terá seu acesso aos recursos de TI suspenso no momento da notificação do distrato. Dados pessoais mantidos em sistemas de armazenamento corporativo deverão ser auditados antes de liberados para no distrato. Contas de acesso serão direcionadas para o gestor da área. Após 60 (sessenta) dias do desligamento, as contas serão apagadas ou anonimizadas.

O prestador de serviço interno que estiver sem contrato ou com ele em vacância com duração superior a 90 (noventa) dias terá direito de acesso aos recursos de TI revogado conforme o regramento interno aplicado ao caso. No caso da vacância, após o período de 90 (noventa) dias, as contas serão apagadas ou anonimizadas e os dados pessoais, se existirem no OneDrive Corporativo, serão apagados.

O acesso a recursos relacionados a sistemas corporativos será provido via perfis de trabalho ou por autorização do gestor da informação envolvida.

É prerrogativa exclusiva da área de TI configurar o compartilhamento de recursos de tecnologia na rede de computadores. Requisições de concessão e alteração de permissões de acesso devem ser encaminhadas à área de tecnologia pela gestão da unidade organizacional interessada.

Na ocorrência da inativação da conta do usuário, seus arquivos armazenados nos recursos de TI poderão ser avaliados pela chefia imediata visando à sua eliminação ou preservação.

3.10. SOBRE OS PROCEDIMENTOS PARA SENHAS DE ACESSO

As senhas de acesso devem ser utilizadas para acesso dos usuários aos sistemas de gestão da Empresa, e-mails, aplicativos, rede de dados etc.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

A solicitação de acesso deve ser realizada através de pedido do líder do usuário para a equipe de TI. Este pedido deve ser feito através de uma requisição registrada no Sistema de Gestão de Serviços de TI.

A partir desta solicitação, a equipe de TI é responsável pela geração da senha e sua entrega ao usuário.

As novas senhas geradas por TI não poderão ser passadas ao solicitante via e-mail. Quando do primeiro acesso pelo usuário, o sistema de segurança das plataformas exige que o próprio usuário modifique a senha fornecida pela Área de TI.

Sobre as responsabilidades do usuário, temos:

- As senhas são pessoais e intransferíveis.
- Será considerada falta grave o uso de senhas compartilhadas.
- As senhas nunca devem ser guardadas em meios eletrônicos como celular, computadores portáteis, mensagens de email etc.
- O usuário pode solicitar a mudança de sua senha a qualquer momento.

Sobre a composição das senhas, as regras são:

- As senhas são compostas por no mínimo 7 (sete) caracteres alfanuméricos, com distinção entre letras maiúsculas e minúsculas, usando caracteres especiais (! @ # $ % & + -), não sendo permitida a repetição seguida de um mesmo caractere.
    - Exemplo 1: tipo incorreto de senha: “abcd99” ou ”aabc98”.
    - Exemplo 2: tipo correto de senha: “S40-P4ul0 ” ou “ $sAo+Paulo% “
- As senhas não podem ser repetidas por um período de 12 meses, ou seja, as plataformas armazenam historicamente as últimas 12 senhas, para fins de controle.

O prazo de expiração das senhas dos usuários, independentemente da plataforma de trabalho, é de 60 dias.

Se o usuário tentar acessar a sua conta com a senha incorreta por mais de 3 vezes, o sistema de gestão de senha do aplicativo (email, rede etc.) poderá bloquear a conta do usuário. Neste caso, a solicitação de desbloqueio deve ser feita pelo líder de equipe do usuário a Área de TI.

Em caso de desligamento, o gestor direto do usuário deve solicitar a TI a revogação dos acessos.

3.11. SOBRE O USO DOS RECURSOS DE ARMAZENAMENTO DE DADOS CORPORATIVOS

Cada área de negócio terá disponível uma área compartilhada para guarda dos arquivos compartilhados entre seus usuários, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança. As áreas privativas e compartilhadas possuem tamanho limitado. Caberá à área de TI definir os limites de armazenamento, de acordo com a disponibilidade.

Os dados armazenados fora das áreas privativa ou compartilhadas não possuem garantias de integridade, disponibilidade, controle de acesso ou cópia de segurança. Por esse motivo, todo produto de trabalho deve ser armazenado no Servidor de Arquivos da Rede.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

A Empresa disponibiliza para o pessoal interno vários tipos de dispositivos de armazenamento de dados. Cada um deles tem um propósito específico. Nesse sentido, o principal elemento de qualificação é o risco associado a perda de informações sensíveis do negócio.

A tabela a seguir apresenta esses recursos e suas aplicações básicas:

Dispositivo de armazenamento	Auditável	Dados corporativos	Dados privados	Compartilhado com clientes (transferência)	Backup Corporativo	Cópia Servidor do Legado
Unidade física (Desktop ou Notebook)	Sim	Sim	Não	Não	Não	Sim
Google Drive Corporativo	Sim	Sim	Não	Não	Não	Sim
Área de arquivos do Onedrive	Sim	Sim	Não	Sim	Sim	Sim
Pendrives	Sim	Não	Sim	Não	Não	Sim
Hd Externo	Sim	Não	Sim	Não	Não	Sim

OBS 1: *O uso de Pendrives e HD Externo para armazenamento de dados corporativos e do negócio (dados de clientes ou Titulares, propostas etc.) é proibido na Empresa. Em situações excepcionais seu uso somente será permitido com a autorização da Diretoria da área responsável e anuência da Diretoria responsável por TI.*

Para garantir o uso organizado desse recurso, a área de TI deverá realizar auditorias anuais com vistas a garantir a conformidade com essas determinações. A desatenção a essas orientações poderá implicar em notificação ou sanções aos líderes de área.

3.12. SOBRE A UTILIZAÇÃO DA REDE SEM FIO E DISPOSITIVOS MÓVEIS

O uso da rede sem fio é destinado a complementar a rede cabeada, possibilitando o acesso diferenciado para os usuários internos e externos aos recursos de TI da Empresa.

O uso da rede sem fio por dispositivos móveis pertencentes a usuários internos ou externos será regulamentado pela área de TI.

Os dispositivos móveis devem ser utilizados considerando-se soluções de segurança, de acordo com a Política de Segurança da Informação da Empresa.

Sobre o acesso à rede corporativa:

a) A rede se conecta automaticamente quando o usuário está na Empresa e pode ser acessada via VPN quando estiver trabalhando remotamente.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

b) Certifique-se de salvar todos os arquivos usados no dia a dia de trabalho na rede. Apenas essas unidades são protegidas pelo backup corporativo.
c) Para criar pastas, solicite suporte.
d) Qualquer pedido de acesso a pastas existentes deve ser feito ao suporte, com cópia para o responsável pela área.
e) Antes de fazer uploads de arquivos pesados para a rede, comunique previamente o suporte.
f) Evite armazenar arquivos pessoais na rede.

3.13. SOBRE A UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

A Empresa dispõe de um endereço eletrônico exclusivo e pessoal para uso regular do seu pessoal interno.

Endereços genéricos, comuns a uma atividade, projeto ou departamento, poderá ser disponibilizado, quando solicitado, para recebimento de mensagens de usuários externos à unidade organizacional.

O usuário que perder o vínculo com a Empresa, permanecer em licença com duração superior a 180 (cento e oitenta) dias terá seu endereço de correio eletrônico excluído e o conteúdo da respectiva caixa postal será mantido conforme normativo interno para esses casos.

3.14. SOBRE O ACESSO À INTERNET

Todos os usuários internos poderão ter acesso à internet, identificados pela sua conta, de uso pessoal e intransferível.

Cabe à área de TI implantar os controles de acesso e mecanismos de auditoria que garantam o monitoramento do acesso à internet pela rede corporativa da Empresa.

Cabe à Diretoria relacionada à área de TI, em conjunto com o Comitê de Segurança da Informação, definir o conteúdo da rede mundial de computadores acessível a partir da rede corporativa da Empresa.

Será bloqueado o acesso a sites de conteúdo considerado ofensivo, ilegal ou impróprio a exemplo de sites pornográficos, de jogos ou apostas.

Os gestores das unidades organizacionais poderão solicitar à área de TI restrição de acesso a sites para os usuários das respectivas unidades.

A área de TI terá acesso aos históricos de utilização da Internet de todos os usuários da Empresa e poderá informá-los aos gestores das respectivas áreas.

3.15. SOBRE O INVENTÁRIO DOS ATIVOS DE TI

Os ativos associados à informação e aos recursos de processamento da informação devem ser inventariados. Entre esses ativos estão relacionados:

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

a) Equipamentos de TI como notebooks, celulares, coletores de dados, desktops, servidores, equipamentos de rede e outros dispositivos usados na operação do negócio;
b) Sistemas, aplicativos e as informações processadas nesses programas.
c) Link de dados, redes de dados, sistema de segurança da informação.
d) Sistemas de armazenamento de arquivos em nuvem etc.

Esses ativos são administrados tendo em vista o Ciclo de Vida da Informação que consiste em criação, processamento, armazenamento, transmissão, exclusão e destruição.

Por meio das Políticas de Privacidade e de Segurança da Informação, bem como pelo conjunto de Procedimentos Corporativos associados a esses assuntos, a área de TI provê uma forma organizada para o uso desses recursos.

Essa organização ajuda a assegurar a proteção efetiva além de atender igualmente outras finalidades, como saúde e segurança, razões de seguro ou financeiras.

3.16. SOBRE OS RECURSOS DE TELEFONIA

A concessão e utilização de linhas telefônicas móveis e aparelhos celulares são providas para facilitar a comunicação dos empregados da Empresa, colaborando para o bom desempenho organizacional.

As linhas e aparelhos de telefonia móvel são considerados equipamentos de trabalho e são distribuídos aos usuários conforme enquadramento dos mesmos nos parâmetros de concessão, que levam em conta as necessidades da empresa x atribuições do cargo ou projeto do usuário.

Assim como em outros dispositivos de computação distribuída, há monitoração pela área de TI e devem ser utilizados apenas para atividades profissionais, uma vez que nestes também não se deve ter expectativa de privacidade.

A concessão do uso se dará conforme as seguintes regras:

a) As atividades do profissional requerem que esteja em movimento entre locais de trabalho na maior parte do tempo da jornada de trabalho ou contrato;
b) Ocupe cargo de confiança, que requeira disponibilidade e prontidão na solução de demandas profissionais, ou
c) Ocupe cargo técnico que requeira disponibilidade em regime de plantões para solução de demandas profissionais.

Quando houver a necessidade de liberação especial, ou seja, fora do contexto definido nesta Política, a mesma deve ser aprovada pela Diretoria do solicitante.

Uso do recurso:

a) Todo usuário que receber o aparelho de telefonia móvel terá a responsabilidade de utilizá-lo racionalmente para o desempenho de suas funções, bem como zelar pela guarda e conservação do aparelho, mantendo-o em segurança e em ótimas condições de uso.
b) O aparelho é para utilização exclusiva do empregado designado, não podendo ser cedido à utilização de terceiros ou uso privado.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

3.17. USO DA ESTAÇÃO DE TRABALHO OU NOTEBOOK

a) A troca e sincronismo de dados entre recursos de computação móvel e computadores da ENGECOMP, ligados à rede ou não, é proibida a menos que o recurso móvel seja de propriedade da mesma e devidamente identificado no inventário da ENGECOMP;
b) É proibido o armazenamento ou processamento de dados da ENGECOMP em computadores ou recursos de informática de propriedade particular;
c) A perda, roubo ou furto de qualquer equipamento móvel de propriedade da ENGECOMP deve ser imediatamente comunicada à área de tecnologia da informação, acompanhada de chamado e boletim de ocorrência policial.
d) Nenhum equipamento poderá ser encaminhado para manutenção sem antes passar pela avaliação e autorização da área de Tecnologia da Informação. Todo equipamento encaminhado para manutenção deve estar sem o disco rígido ou a manutenção deve ser realizada na própria empresa com acompanhamento da área de Tecnologia da Informação ou alguém designado.
e) Nenhum equipamento poderá ser reposto sem antes passar pela avaliação e autorização da área de Infraestrutura de TI.
f) Evite utilizar a máquina em superfícies inadequadas, como sofás, camas e colo, assim como superfícies estofadas.
g) Mantenha a higiene do equipamento; evite comer enquanto o utiliza e previna o acúmulo de poeira.
h) Não armazene o equipamento próximo a produtos líquidos.
i) Evite deixar garrafas de água abertas ou canecas com líquidos próximos ao notebook.
j) Evite deixar o equipamento em superfícies propensas a quedas.
k) Ao transportar o equipamento, segure-o com ambas as mãos para evitar quedas.
l) Desligue o equipamento ao final do expediente, diariamente.
m) Sempre que o sistema solicitar uma atualização, entre em contato coma área de suporte de TI.
n) Use a máquina na tomada apenas para carregar completamente a bateria.

3.18. USO DE APLICATIVOS DE COMUNICAÇÃO

Serviço de mensageria eletrônica por meio do aplicativo “WhatsApp” e/ou “WhatsApp Web”, é homologado pela área de TI. Tal serviço destina-se à postagem de vídeos, gravações de áudio, fotografias, textos e arquivos em geral, doravante denominados “Material”, com o propósito de desempenhar exclusivamente as atividades para as quais foi contratado, ou seja, no estrito interesse da ENGECOMP

Aplicam-se ao uso desses recursos os termos e condições estabelecidos nas Políticas de Segurança da Informação e Privacidade de Dados.

A ENGECOMP se reserva o direito de suspender ou cancelar o acesso à ferramenta, a seu exclusivo critério e a qualquer tempo, independente de aviso prévio ao colaborador.

Nenhum dado de pessoal ou sensível de clientes ou associados a qualquer contrato da ENGECOMP com seus clientes ou fornecedores pode ser trafegado por meio do aplicativo WhatsApp ou similares. Esses dados podem ser transacionados exclusivamente por meio da área de transferência do Sharepoint. Exceções somente serão aceitas por meio de transferência por e-mail com anuência da diretoria da área relacionada.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

3.19. TRANSFERÊNCIA, COMPARTILHAMENTO E MANUSEIO DE DADOS

O Onedrive é o meio oficial e primário de tráfego de dados de titulares entre a Empresa e seus clientes. Clientes que formalizem por contrato meios alternativos como e-mail, Teams, Serviço Amazon S3 ou compatível também são homologados na Empresa, porém seu uso deve ser comunicado a área de TI. Meios diferentes de transferência de dados de titulares devem ser aprovados e liberados pela área de TI.

Internamente, de modo geral, os dados de titulares devem ser manuseados com cautela. O documento **"Procedimento para Manuseio de Dados Pessoais" deve** ser observado. Esse documento estabelece as regras gerias para o manuseio de dados considerando os seguintes itens:

- **FINALIDADE**: O manuseio de dados pessoais deve ser realizado unicamente para o cumprimento de uma finalidade específica, pré-determinada e informada ao titular;
- **NECESSIDADE:** O manuseio deve ser restrito ao mínimo de dados pessoais necessário para o alcance da finalidade pré-definida;
- **NÃO DISCRIMINAÇÃO:** O manuseio de dados pessoais não pode ser realizado para fins discriminatórios ilícitos;
- **QUALIDADE:** A empresa deve se atentar para a precisão, qualidade e acurácia dos dados que manuseia.
- **TRANSPARÊNCIA:** DEVE ser garantida a transparência ao titular sobre o tratamento de seus dados pessoais.
- **COMPARTILHAMENTO DE DADOS PESSOAIS:** Ao compartilhar Dados Pessoais com Terceiros, (enviar ou receber dados), devem ser observadas as regras estabelecidas no Procedimento de Compartilhamento de Dados Pessoais.
- **ARMAZENAMENTO DE DADOS PESSOAIS:** Os documentos que contenham Dados Pessoais não podem ser armazenados por período superior ao necessário para o cumprimento da finalidade pretendida, independentemente do formato utilizado, se físico ou eletrônico.
- **DADOS PESSOAIS SENSÍVEIS**: No manuseio de dados pessoais sensíveis, deve ser observadas as hipóteses autorizadoras específicas para tanto, conforme exposto mais adiante neste texto.

O compartilhamento de dados de titulares é uma atividade comum no negócio da Empresa, no entanto, essa atividade é regulada por meio das instruções do documento "Procedimentos de Compartilhamento de Dados".

A Empresa determina regras específicas para o compartilhamento de Dados Pessoais, considerando o nível de sensibilidade da operação. Deverão ser observadas para cada nível de sensibilidade as seguintes regras:

- **Compartilhamento de dados sem identificação dos titulares.** Este tipo de compartilhamento é liberado desde que os dados sejam anonimizados ou a identificação do titular seja impossível.
- **Compartilhamento de dados para cumprimento de contrato ou mandamento legal.** O Gestor da Área Solicitante/Responsável pelo compartilhamento deve solicitar via e-mail ou sistema de chamados designado pela área de TI, uma solicitação de avaliação da criticidade do evento ou processo. Este procedimento vai submetê-lo para a avaliação e aprovação do DPO.
- **Compartilhamento de Dados Pessoais para país estrangeiro ou organismo internacional.** Como nos outros casos esse tipo de compartilhamento deve ser submetido a avaliação da área de TI.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

3.20. DESCARTE OU ELIMINAÇÃO DE DADOS OU EQUIPAMENTOS

A Empresa estabelece uma sistemática para o processo de descarte de equipamentos de Tecnologia da Informação excedentes e a higienização dos dados desses equipamentos. O documento "Procedimentos de Destruição e Descarte de Equipamentos Eletrônicos e Dados Pessoais e Sensíveis" deve ser observado obrigatoriamente.

Cada dispositivo deve ser avaliado para determinar se o dispositivo deve ser higienizado ou se os dados no dispositivo precisam ser retidos e transferidos entre as áreas da Empresa.

Nenhum registro contendo dados pessoais ou dados sensíveis de usuários, terceiros ou clientes, deve ser descartado, a menos que a sanitização a seguir seja realizada:

- Destruição das informações de identificação pessoal contidas no registro; ou
- Modificação do registro para tornar as informações de identificação pessoal ilegíveis; ou
- Observação das instruções da metodologia de sanitização de TI da Empresa.
- Os dados que devem ser retidos e transferidos para um novo dispositivo devem ser feitos sob consulta com a equipe de suporte de TI ou de Privacidade.

3.20.1. PROCEDIMENTOS EM CASOS DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Em eventos de segurança o documento "Procedimento Corporativo para Resposta a Incidentes de Segurança da Informação e Privacidade de Dados Pessoais" deve ser considerado. Ele estabelecer a sistemática para o processo de resposta a Incidentes de segurança de Dados Pessoais na Empresa.

Em caso de Incidentes, a resposta adequada será fundamental para a minimização dos danos causados aos Titulares dos Dados afetados e à Empresa.

Os usuários devem relatar prontamente qualquer comportamento ou circunstância suspeita que indique a violação de Dados Pessoais. Caso perceba alguma anormalidade ou evento que configure um Incidente, o Colaborador deve:

- Tomar nota dos eventos que o levaram a acreditar que um Incidente esteja ocorrendo (data, hora, sistemas, computador ou pessoas afetadas/envolvidas);
- Notificar imediatamente ao Encarregado pela Proteção de Dados Pessoais, por meio do e-mail dpo@engecomp.com.br

O DPO deve monitorar estes canais e fazer a análise inicial dos reportes recebidos, de forma imediata, juntamente com o suporte da área jurídica e da Diretoria da Empresa.

3.21. PROPRIEDADE INTELECTUAL

Os produtos de trabalho dos processos de negócio da Empresa podem gerar artefatos protegidos por direitos autorais (textos, desenhos, programas de computador etc.) ou propriedade industrial (marcas, patentes, segredo industrial etc.)

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

A área de TI é comprometida com a gestão da Propriedade Intelectual da Organização com o objetivo de benefício da liderança comercial e tecnológica da Empresa. Nesse sentido as regras preconizadas pela Lei da Propriedade Industrial (Lei nº 9.279/96) e pela Lei do Software, a Lei n.º 9.609/98 que assegura ao criador do software a mesma proteção da propriedade intelectual endossada aos autores de obras literárias, são endereçadas nos trabalhos e contratações de TI.

A pirataria de software é proibida na Empresa. A área de TI deve ser informada caso algum usuário perceba a utilização de programas de computador com suspeitas de pirata.

Anualmente a área de TI realizará auditoria com vistas a identificar e bloquear o uso de softwares piratas.

3.22. LICENCIAMENTO, DISTRIBUIÇÃO E USO DE SOFTWARE

Qualquer software desenvolvido ou independentemente de sua condição comercial, deve ser homologado e implementado pela área de tecnologia da informação.

Todo o software que estiver sujeito à legislação local de direitos autorais, Open Source deve ser avaliada e viabilizada pela área de Tecnologia da Informação.

Será considerada infração e passível de sanções a utilização e instalação de softwares não aprovados pela área de TI.

São proibidas cópias não autorizadas de software licenciados ou de propriedade da Empresa, seja para uso pessoal ou para terceiros.

3.23. COMPROMISSO COM INOVAÇÃO PARA MELHORIA DOS PROCESSOS DE NEGÓCIO

Em linha com as estratégias globais da Empresa a área de TI opera de forma engajada com o compromisso de aprimorar o relacionamento e gestão dos sistemas com vistas a temas como sustentabilidade e inovação.

São considerados em âmbito operacional da área de TI critérios de sustentabilidade na contratação, treinamento e engajamento em práticas de sustentabilidade.

3.24. PENALIDADES

É exigido a todos os usuários da Empresa o cumprimento das determinações apresentadas neste documento, constituindo violação a não observância dos preceitos nela descritos, podendo acarretar a aplicação de medidas disciplinares tais como advertência verbal, escrita e até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida aos Colaboradores próprios e ainda, penalidades contratuais aos prestadores de serviços ou clientes que descumpram estas regras. Toda infração será avaliada pela área de TI, Gestão de Pessoas e Dep. Jurídico, através da instauração de sindicância interna e apuração do ocorrido e na sequência as medidas legais serão devidamente tomadas em face aos envolvidos.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

4. POLÍTICA DE RESPOSTA A INCIDENTES

4.1. OBJETIVO

Este procedimento tem como propósito estabelecer a sistemática para o processo de resposta a incidentes de segurança da informação e privacidade de dados pessoais na ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”. Este documento visa garantir uma resposta eficaz e eficiente a incidentes, minimizando os danos aos titulares dos dados e à Empresa, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis, bem como com as normas ISO 27002 e ISO 27035.

4.2. ESCOPO

Este procedimento se aplica a todos os usuários internos, terceiros, parceiros, fornecedores e outras partes interessadas que tenham acesso a dados pessoais e informações da ENGECOMP. Abrange todos os sistemas, redes, dispositivos e processos que armazenam, processam ou transmitem dados pessoais e informações confidenciais da Empresa.

4.3. REFERÊNCIAS

- Lei Geral de Proteção de Dados (LGPD)
- ISO/IEC 27002:2022 - Código de prática para controles de segurança da informação
- ISO/IEC 27035 - Gestão de incidentes de segurança da informação
- Política de Segurança da Informação da ENGECOMP
- Política de Privacidade de Dados Pessoais da ENGECOMP
- Política de Uso de Recursos de TI da ENGECOMP
- Procedimento de Gestão da Segurança da Informação da ENGECOMP
- Responsabilidades do Encarregado pela Privacidade de Dados da ENGECOMP
- Catálogo de Serviços de Privacidade da ENGECOMP

4.4. EQUIPE DE RESPOSTA A INCIDENTES (CSIRT)

Na Empresa os seguintes atores devem compor a equipe de Respostas a Incidentes:

a) Responsável pela Segurança da Informação (CISO)
b) Responsável pela Privacidade de Dados (DPO)

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

c) Responsável pela aplicação e sistemas (CTO)
d) Consultor Jurídico
e) Membro executivo do Comitê de Privacidade e Proteção de Dados.

Esta equipe deve ser acionada pelo CISO ou DPO sempre que necessário e de forma tempestiva.

4.5. FASES DE UM INCIDENTE DE PRIVACIDADE DE DADOS

Em caso de Incidentes, a resposta adequada será fundamental para a minimização dos danos causados aos Titulares dos Dados afetados e à Empresa. A resposta a incidentes de segurança da informação e privacidade de dados pessoais deve seguir as seguintes fases:

a) **Preparação:** Estabelecimento de políticas, procedimentos, ferramentas e recursos para lidar com incidentes.

b) **Detecção e Relato:** Identificação e comunicação de eventos suspeitos ou incidentes confirmados.

c) **Análise e Classificação:** Avaliação do impacto e criticidade do incidente.

d) **Contenção:** Ações para limitar o escopo e o impacto do incidente.

e) **Erradicação:** Remoção da causa raiz do incidente.

f) **Recuperação:** Restauração dos sistemas e dados afetados ao estado normal de operação.

g) **Análise Pós-Incidente:** Documentação das lições aprendidas e implementação de melhorias.

4.5.1. PREPARAÇÃO

A fase de preparação é crucial para garantir uma resposta eficaz a incidentes. As seguintes atividades devem ser realizadas:

- **Desenvolvimento e Manutenção de Políticas e Procedimentos:**
    - Este procedimento de resposta a incidentes deve ser documentado, revisado e atualizado regularmente.
    - As Políticas de Segurança da Informação e Privacidade de Dados devem ser sincronizadas com esse documento.
- **Implementação de Ferramentas e Tecnologias:**

  Sob a responsabilidade do CISO os seguintes recursos devem ser considerados:
    - Ferramentas de detecção de intrusão (IDS) e prevenção de intrusão (IPS).
    - Sistemas de gerenciamento de eventos e informações de segurança (SIEM).
    - Software antivírus e antimalware.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Ferramentas de análise forense.
- Sistemas de backup e recuperação de dados.

- **Conscientização e Treinamento:**

  O calendário de eventos deve ser coordenado pelo DPO em alinhamento com o Diretor da equipe Digital. Deve considerar os seguintes objetivos:

  - Treinar os usuários internos sobre como identificar e relatar incidentes.
  - Realizar simulações de incidentes para testar a eficácia dos procedimentos.
  - Promover a conscientização sobre segurança da informação e privacidade de dados.

4.5.2. DETECÇÃO

A detecção e o relato oportunos de incidentes são essenciais para minimizar os danos. As seguintes diretrizes devem ser seguidas:

- **Monitoramento:**
  - A Empresa deve implementar mecanismos de monitoramento para detectar atividades suspeitas ou anormais em seus sistemas e redes.
  - O monitoramento deve ser contínuo e abranger todos os ativos de informação relevantes.
  - As ferramentas de monitoramento devem ser configuradas para gerar alertas em caso de eventos suspeitos.
- **Exemplos de Incidentes:**
  - Perda ou roubo de dispositivos contendo dados pessoais.
  - Acesso não autorizado a sistemas ou dados.
  - Ataques de malware (vírus, ransomware, spyware).
  - Ataques de phishing ou engenharia social.
  - Vazamento de dados (divulgação não autorizada de informações).
  - Negação de serviço (DoS) ou ataques distribuídos de negação de serviço (DDoS).
  - Uso indevido de recursos de TI.
  - Falhas de segurança em aplicativos ou sistemas.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

4.5.3. REPORTE DE POSSÍVEIS INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

Os usuários internos devem relatar prontamente qualquer comportamento ou circunstância suspeita que indique a violação de Dados Pessoais. Caso perceba alguma anormalidade ou evento que configure um Incidente, o usuário deve:

- Tomar nota dos eventos que o levaram a acreditar que um Incidente esteja ocorrendo (data, hora, sistemas, computador ou pessoas afetadas/envolvidas);
- Notificar imediatamente ao Encarregado pela Proteção de Dados Pessoais, por meio do e-mail dpo@engecomp.com.br

O Encarregado deve monitorar estes canais e fazer a análise inicial dos reportes recebidos, de forma imediata, juntamente com o gestor da área de Segurança da Informação.

Reportes externos também deverão ser analisados pelo Encarregado e pelo gestor da área de Segurança da Informação.

Contratos com Terceiros que disponham sobre a necessidade de notificar um Incidente de violação de Dados Pessoais à Empresa devem prever os canais acima descritos para o reporte, sem prejuízo de outros que possam vir a ser instituídos pelas partes contratualmente.

Evite tomar ações arbitrárias como remover arquivos desconhecidos ou reinicializar o sistema. Nenhuma tentativa de correção do problema deve ser feita por um Usuário, a menos que sob direta orientação do Service Desk ou área de Segurança da Informação;

Na ocorrência de um vírus não removível pela vacina instalada, os Usuários de desktops ou notebooks devem desligar o equipamento para evitar a propagação dos danos e entrar em contato imediatamente com o Service Desk.

4.5.4. ANÁLISE E CLASSIFICAÇÃO

Após o relato de um incidente, a equipe de resposta a incidentes deve realizar uma análise para determinar sua natureza, escopo e impacto. As seguintes atividades devem ser realizadas:

- **Avaliação Inicial:**
  - Verificar a validade do incidente.
  - Coletar informações adicionais sobre o incidente.
  - Determinar os sistemas e dados afetados.
  - Avaliar o impacto potencial do incidente.
- **Classificação do Incidente:**
  - Os incidentes devem ser classificados com base em sua gravidade e impacto nos negócios.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- A classificação deve considerar fatores como confidencialidade, integridade e disponibilidade dos dados, bem como requisitos legais e regulatórios.
- A seguinte escala de classificação pode ser usada:
  - **Baixa:** Incidente com impacto mínimo nos negócios e nos titulares dos dados.
  - **Média:** Incidente com impacto moderado nos negócios e nos titulares dos dados.
  - **Alta:** Incidente com impacto significativo nos negócios e nos titulares dos dados, podendo resultar em danos financeiros, reputacionais ou legais.
  - **Crítica:** Incidente com impacto severo nos negócios e nos titulares dos dados, podendo interromper as operações da Empresa ou resultar em violações graves da LGPD.

- **Priorização:**
  - Os incidentes devem ser priorizados com base em sua classificação e impacto nos negócios.
  - Incidentes de alta e crítica prioridade deve ser tratados imediatamente.

4.5.5. CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Após a análise e classificação, a equipe de resposta a incidentes deve tomar medidas para conter o incidente, erradicar a causa raiz e recuperar os sistemas e dados afetados. As seguintes atividades devem ser realizadas:

- **Contenção:**
  - Isolar os sistemas afetados para evitar a propagação do incidente.
  - Desativar contas de usuário comprometidas.
  - Bloquear endereços IP ou domínios maliciosos.
  - Implementar medidas de segurança adicionais para proteger os sistemas.
- **Erradicação:**
  - Identificar e remover a causa raiz do incidente (por exemplo, malware, vulnerabilidades de software).
  - Aplicar patches de segurança ou atualizações de software.
  - Reforçar as medidas de segurança para evitar futuros incidentes.
- **Recuperação:**
  - Restaurar os sistemas e dados afetados a partir de backups.
  - Verificar a integridade dos dados restaurados.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Monitorar os sistemas recuperados para garantir que o incidente não se repita.

4.5.6. ANÁLISE PÓS-INCIDENTE

Após a resolução do incidente, a equipe de resposta a incidentes deve realizar uma análise pós-incidente para identificar as lições aprendidas e implementar melhorias nos procedimentos de resposta a incidentes e nas medidas de segurança. As seguintes atividades devem ser realizadas:

- **Documentação:**
  - Documentar todos os aspectos do incidente, incluindo a causa raiz, as ações tomadas para conter, erradicar e recuperar, o impacto nos negócios e as lições aprendidas.
- **Análise da Causa Raiz:**
  - Realizar uma análise detalhada da causa raiz do incidente para identificar as vulnerabilidades ou falhas de segurança que permitiram que ele ocorresse.
- **Identificação de Lições Aprendidas:**
  - Identificar as lições aprendidas com o incidente, incluindo o que foi feito bem e o que pode ser melhorado.
- **Implementação de Melhorias:**
  - Implementar as melhorias identificadas nos procedimentos de resposta a incidentes, nas medidas de segurança, nos treinamentos e na conscientização dos usuários internos.
- **Relatório Pós-Incidente:**
  - Preparar um relatório pós-incidente para a alta administração e outras partes interessadas relevantes, resumindo o incidente, as ações tomadas, o impacto nos negócios e as lições aprendidas.

4.5.7. CLASSIFICAÇÃO DA CRITICIDADE

Constatada a ocorrência de um Incidente, o Encarregado, com os insumos fornecidos pelo gestor da área de Segurança da Informação, deve classificar o Incidente conforme a sua criticidade.

Classificados os Dados Pessoais envolvidos, a Criticidade deve ser avaliada, conforme tabela 2, abaixo.

A comunicação da ocorrência de um Incidente à ANPD e aos Titulares dos Dados afetados é obrigatória quando a criticidade do Incidente tiver sido classificada como média ou alta.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Tabela 2 – Grau de Criticidade do Incidente

Classificação dos Dados	Grau de criticidade do Incidente	Risco ou dano ao Titular	Notificação do Incidente
Simples	Baixa	Irrelevante	Não
Financeiros e/ou Comportamentais, combinados ou não com Dados Simples	Média	Relevante	Sim
Sensíveis (combinados ou não com outros tipos de Dados)	Alta	Relevante	Sim

4.5.8. CLASSIFICAÇÃO DOS DADOS

Para fins de identificação do grau de criticidade de um Incidente, os Dados Pessoais devem ser previamente classificados, de acordo com as seguintes definições:

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Tabela 1 – Classificação dos Dados

Classificação dos Dados	Descrição
Simples	Quaisquer informações relativas a uma pessoa singular identificada ou identificável, e que não esteja classificada abaixo como Dados Financeiros e/ou Comportamentais.
Financeiro	Dados pessoais que que remetam ou revelem qualquer aspecto da vida financeira do Titular. Exemplos: número de conta, cartão de crédito, código verificador, renda, salário, benefícios.
Comportamentais	Dados pessoais que demonstrem ou revelem o comportamento do Titular. Exemplos: Dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.
Sensíveis	Dados Pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, Dado genético ou biométrico, quando vinculados a uma pessoa natural.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

4.6. NOTIFICAÇÃO DO INCIDENTE

O Encarregado deve notificar o Incidente para a ANPD e para os Titulares, quando cabível.

4.7. RESPONSABILIDADES

É responsabilidade de todos os usuários internos:

- Conhecer, entender e aderir às regras descritas neste documento;
- Conhecer suas responsabilidades descritas neste documento;
- Reportar qualquer suspeita de Incidente.

É responsabilidade do Encarregado:

- Receber e analisar as notificações de incidentes;
- Manter as evidências de todos os passos adotados nos casos de resposta ao Incidente e arquivamento de reportes;
- Nos casos de Incidente, elaborar relatório que conste, no mínimo:
    a) A causa raiz do Incidente;
    b) Medidas adotadas para a resposta ao Incidente;
    c) Tempo de reação entre a descoberta do Incidente e o início do seu gerenciamento;
    d) Notificações e comunicações efetuadas sobre o Incidente;
    e) Impacto financeiro, reputacional e operacional do Incidente, na Empresa.
    f) Classificar, com os insumos fornecidos pelo gestor da área de Segurança da Informação, o nível de criticidade do Incidente;
    g) Coordenar todos os posicionamentos públicos e estratégias processuais (administrativos ou judiciais), relativos ao Incidente, quando cabível.

É responsabilidade do Comitê de Privacidade e Proteção de Dados:

- Aprovar os posicionamentos públicos e estratégicos, relativos ao Incidente;
- Alinhar o posicionamento e protocolos com todos os heads responsáveis das áreas de negócio.

É responsabilidade do gestor da área de Segurança da Informação:

- Cessar a fonte de vazamento, se for o caso;
- Realizar a análise técnica do Incidente;
- Realizar a detecção, isolamento, remoção e preservação dos sistemas afetados;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Garantir que as evidências sejam mantidas para posterior perícia técnica;
- Contratar assessoria externa para apoiar em questões técnicas, se necessário;
- Auxiliar no levantamento das informações técnicas que deverão compor as notificações e comunicados a serem emitidos pela empresa.

É responsabilidade da área jurídica:

- Revisar todas as notificações de comunicação do Incidente à ANPD e aos Titulares dos Dados;
- Auxiliar no posicionamento público da Empresa sobre o Incidente, perante a imprensa, o mercado, usuários internos e parceiros da empresa;
- Identificar obrigações contratuais e regulatórias de reportar o Incidente para Terceiros, órgãos reguladores/governamentais (que não a ANPD), elaborar e enviar as respectivas notificações;
- Auxiliar na elaboração de estratégias de compensação aos Titulares de Dados afetados, quando tal ação for necessária;
- Contratar assessoria externa jurídica, quando necessário, para apoio e consultoria para a resposta ao Incidente.

É responsabilidade do gestor da equipe de Digital:

- Identificar o impacto do Incidente no relacionamento com as partes interessadas internas;
- Auxiliar na elaboração e divulgação das comunicações internas, quando necessárias.

O Diretor Executivo deverá:

- Aprovar o posicionamento da empresa sobre o Incidente, quando o mesmo repercutir na imprensa;
- Atuar como porta-voz da empresa sobre o Incidente, quando necessário.

4.8. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo canal dpo@engecomp.com.br

O cumprimento deste Procedimento é de suma importância e dever de todos. Em caso de não observância deste Procedimento, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: dpo@engecomp.com.br

As denúncias de violações às Políticas e Procedimentos serão anônimas e a não-retaliação será garantida.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

5. POLÍTICA DE GESTÃO DO SEGURANÇA DA INFORMAÇÃO (SGSI)

5.1. OBJETIVO

Estabelecer a sistemática para o Sistema de Gestão de Segurança da Informação (SGSI) junto a ENGECOMP ltda e suas controladas, coligadas e sob controle comum ("Empresa").

5.2. ABRANGÊNCIA

Este documento é destinado à:

- Gerência sênior, que tomam decisões sobre o orçamento de segurança da informação.
- Gerente da Segurança da Informação, que implementa o programa de segurança.
- Especialistas e coordenadores de segurança da informação, que são responsáveis pelas ações relativas à segurança da informação.
- Donos de sistemas, responsáveis diretos pelas informações.
- Equipe de suporte técnico (por exemplo, rede, sistema, aplicativo e administradores de banco de dados; especialistas de infraestrutura, analistas de segurança de dados), que gerenciam e administram a segurança dos sistemas da informação.
- Programadores de sistema e aplicativos, que desenvolvem e mantêm os códigos que podem afetar o sistema e integridade dos dados
- Auditores e pessoal da qualidade de sistema de informação, que garantem o baseline das especificações de segurança dos sistemas da informação.

5.3. TERMOS E DEFINIÇÕES

- **Administrador de Segurança**: significa o funcionário com privilégios especiais, responsável por efetuar administração de usuários;
- **Backup:** significa cópia de segurança de arquivos, mídias, papéis, ou qualquer outra fonte de informação;
- **Classificação da Informação:** significa o processo através do qual o Proprietário da Informação atribui um grau de sigilo às informações;
- **Comunicação eletrônica:** significa todo o meio eletrônico utilizado para o envio e recebimento de dados, esteja ele restrito ou não ao perímetro corporativo da Empresa e Empresa e das suas empresas controladas e subsidiária integral. As comunicações eletrônicas incluem, mas não se limitam a: correio eletrônico, correio de voz, videoconferência, acesso à internet (seja web ou qualquer outro tipo de protocolo) e intranet;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Criptografia**: significa métodos de proteção de informações pelos quais apenas os detentores de um determinado segredo denominado "chave", têm acesso a elas. Informações criptografadas, mesmo quando capturadas em trânsito pela rede, não podem ser lidas por quem não conhece a chave necessária;
- **Custodiante:** pessoa responsável zelar pelo armazenamento e preservação de informações que não lhe pertencem no qual lhe são permitidos o direito.
- **Gestor da Informação:** significa a pessoa responsável pelo Departamento e/ou Processo de Negócio onde a informação foi gerada ou o primeiro receptor ou manipulador da informação;
- **Gestor de sistema:** significa a pessoa responsável pelo departamento e/ou processo de negócio que seja o principal usuário das informações manipuladas pelo sistema;
- **Grau de Sigilo:** significa a grau atribuída a ativos de informação considerados sigilosos em decorrência da sua natureza ou conteúdo;
- **Informação:** significa os recursos de informação que são definidos como qualquer dado criado, coletado, comunicado, usado ou observado por qualquer usuário de informação durante o seu período empregatício ou relacionamento com a Empresa e suas empresas controladas e subsidiária integral;
- **Notebook / laptop**: significa computador portátil;
- **Rede Interna:** Credenciais de acessa a rede de computadores da Empresa.
- **Sistemas:** significa quaisquer sistemas de computação, aplicativos (App), plataformas e/ou redes de dados que tratam dados corporativos.
- **Sigilo:** significa segredo de conhecimento restrito a pessoas credenciadas, proteção contra revelação não-autorizada; e

5.4. PAPEIS E RESPONSABILIDADES

Sobre as responsabilidades associadas a gestão da segurança da informação e seus atores, temos o seguinte:

Diretor executivo da Empresa:

a) Habilitar o orçamento para SI.

b) Atuar em conjunto com o Comitê Consultivo de SI.

c) Ser a última instância de aprovação para projetos de grande porte em SI.

Comitê Consultivo de Segurança da Informação e Mudanças (CCSIM):

a) Definir o escopo e os limites do SGSI em termos das características da empresa, da Empresa, de sua localização, ativos e tecnologia.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

b) Analisar e aprovar um SGSI de acordo com a política da empresa e alinhado com a empresa, a Empresa, sua localização, ativos e tecnologia.

Gerente Segurança da Informação:

a) Incluir detalhes e justificativas para quaisquer exclusões do escopo.

b) Definir um SGSI de acordo com a política da empresa e alinhado com a empresa, a Empresa, sua localização, ativos e tecnologia.

c) Alinhar o SGSI com a abordagem corporativa geral para o gerenciamento de segurança.

d) Obter autorização de gestão para implementar e operar ou alterar o SGSI.

e) Aprovar revisões regulares da eficácia do SGSI, incluindo o cumprimento da política e dos objetivos do SGSI e a revisão das práticas de segurança.

f) Preparar e manter uma declaração de aplicabilidade que descreva o escopo do SGSI.

g) Definir e comunicar as funções e responsabilidades de gerenciamento de segurança da informação.

h) Comunicar a abordagem ISMS.

i) Formular e manter um plano de tratamento de riscos de segurança da informação alinhado com os objetivos estratégicos e a arquitetura corporativa.

j) Certifique-se de que o plano identifique as práticas de gerenciamento e soluções de segurança apropriadas e ideais, com recursos, responsabilidades e prioridades associados para gerenciar o risco de segurança da informação identificado.

k) Recomendar programas de treinamento e conscientização sobre segurança da informação.

l) Integrar o planejamento, desenho, implementação e monitoramento de procedimentos de segurança da informação e outros controles capazes de permitir a pronta prevenção, detecção de eventos de segurança e resposta a incidentes de segurança.

m) Realizar auditorias internas de SGSI em intervalos planejados.

n) Realizar uma revisão gerencial do SGSI regularmente para garantir que o escopo permaneça adequado e que as melhorias no processo do SGSI sejam identificadas.

Equipe de Segurança da Informação

a) Manter como parte da arquitetura corporativa um inventário de componentes da solução que estão em vigor para gerenciar riscos relacionados à segurança.

b) Desenvolver propostas para implementar o plano de tratamento de riscos de segurança da informação, apoiados por casos de negócios adequados, que incluem a consideração de financiamento e alocação de funções e responsabilidades.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

c) Fornecer informações para o design e desenvolvimento de práticas e soluções de gerenciamento selecionadas do plano de tratamento de riscos de segurança da informação.

d) Defina como medir a eficácia das práticas de manejo selecionadas e especifique como essas medições devem ser usadas para avaliar a eficácia para produzir resultados comparáveis e reprodutíveis.

e) Realizar revisões regulares da eficácia do SGSI, incluindo o cumprimento da política e dos objetivos do SGSI e a revisão das práticas de segurança.

f) Considerar os resultados das auditorias de segurança, incidentes, resultados de medições de eficácia, sugestões e feedback de todas as partes interessadas.

g) Fornecer informações para a manutenção dos planos de segurança para levar em consideração as conclusões das atividades de monitoramento e revisão.

h) Registrar ações e eventos que possam ter impacto na eficácia ou no desempenho do SGSI.

5.5. PROCEDIMENTOS PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO.

Para manter a integridade da informação e proteger os ativos de TI, uma série de atividades são desempenhados. Este conjunto e atividades (ou rotinas) é descrito a seguir com indicação inclusive de metas e métricas para gestão dessas rotinas.

O conjunto inclui atividades que tratam desde o estabelecimento e a manutenção de papéis e responsabilidades até procedimentos de segurança de TI e ações corretivas das deficiências ou dos incidentes de segurança.

5.5.1. PLANEJAMENTO DA SEGURANÇA DA INFORMAÇÃO

Programa de Segurança de TI e Garantia da Privacidade de dados.

O responsável pelos serviços de Segurança da Informação deve traduzir os requisitos de negócio, de risco e conformidade, em um programa abrangente de segurança de TI e Privacidade de dados.

Deve também garantir o atendimento de requisitos de infraestrutura de TI, da cultura de segurança e os requisitos da LGPD para o negócio.

Definição de Incidente de Segurança.

Deve ser definido e comunicado claramente as características de incidentes de segurança em potencial para que possam ser tratados adequadamente pelos processos de gestão de incidentes ou gestão de problemas.

As definições de incidentes devem levar em consideração especial os requisitos legais como declarados nas cláusulas de conformidade com a LGPD. Para atender este requisito, estas definições devem ser alinhadas com a área de Privacidade.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

5.5.2. GESTÃO DA SEGURANÇA DE TI

O responsável pela Segurança da Informação deve gerenciar a segurança de TI no mais alto nível organizacional da empresa de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio. Os seguintes são os procedimentos operacionais essenciais ao negócio:

- **Gestão de Identidade.**
    a) Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo.
    b) Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados.
- **Gestão de Contas de Usuário.**
    a) Deve assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário.
    b) Esse procedimento deve ser aplicado a todos os usuários, inclusive aos administradores (usuários com privilégios), usuários internos e externos, para os casos normais ou emergenciais.
- **Gestão contas de superusuário ou administradores locais**
    a) Acessos com privilégios especiais, como perfil administrador ou superusuário, devem ter condições de uso e responsabilização descritas em cláusulas nos contratos de usuários e de serviços que especifiquem as sanções em caso de tentativa de acesso não autorizado pelos usuários ou por terceiros. Tais perfis devem ser restritos e controlados.
    b) Sistemas de multiusuários que necessitam de proteção contra acesso não autorizado devem ter a concessão de privilégios controlada por um processo de autorização formal. Este processo deve considerar as seguintes diretrizes:
        - Deve ser identificado claramente privilégio de acesso de cada produto de sistema, por exemplo, sistema operacional, sistemas de gerenciamento de banco de dados e cada aplicação e de categorias de usuários para os quais estes necessitam ser concedido;
        - Os privilégios sejam concedidos a usuários conforme a necessidade de uso e com base em eventos alinhados com as diretrizes da Empresa para controle de acesso, por exemplo, requisitos mínimos para sua função somente quando necessário;
        - O processo de autorização e um registro de todos os privilégios concedidos devem ser documentados por meio eletrônico na ferramenta oficial da Empresa para esse fim;
        - Os ID de usuários com privilégios especiais devem ser distintos daqueles usados normalmente para os negócios.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Gestão de Chave Criptográfica.**

  a) Deve assegurar que sejam estabelecidos políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada.

  b) As chaves criptográficas devem ser protegidas contra modificação, perda e destruição. Adicionalmente, chaves secretas e privadas devem ser protegidas contra a divulgação não autorizada.

  c) O sistema de gerenciamento de chaves deve ser baseado em um conjunto estabelecido de normas e documentado de forma exclusiva em uma Procedimento Padrão ou Instrução Técnica. Essas instruções devem descrever meios seguros para:

    - gerar chaves para diferentes sistemas criptográficos e diferentes aplicações;
    - gerar e obter certificados de chaves públicas;
    - distribuir chaves para os usuários devidos, incluindo a forma como as chaves devem ser ativadas;
    - armazenar chaves, incluindo a forma como os usuários autorizados obtêm acesso a elas;
    - mudar ou atualizar chaves, incluindo regras relativas à quando as chaves devem ser mudadas e como isto será feito;
    - lidar com chaves comprometidas;
    - revogar chaves, incluindo regras de como elas devem ser retiradas ou desativadas, por exemplo quando chaves tiverem sido comprometidas ou quando um usuário deixa a Empresa (convém que, também neste caso, que as chaves sejam guardadas);
    - recuperar chaves perdidas ou corrompidas, como parte da gestão da continuidade do negócio, por exemplo para recuperação de informações cifradas;
    - guardar chaves, por exemplo para informações guardadas ou armazenadas em cópias de segurança;
    - destruir chaves;
    - manter registro e auditoria das atividades relacionadas com o gerenciamento de chaves.

- **Proteção da Tecnologia de Segurança.**

  a) Deve garantir que as tecnologias de segurança importantes sejam invioláveis e que as documentações de segurança não sejam reveladas desnecessariamente.

  b) Deve garantir que exista um inventário completo e atualizado dos ativos de informação para a gestão efetiva de vulnerabilidade técnica.

  c) Deve garantir o controle sobre acesso ou tentativas de acesso aos dispositivos de segurança.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

d) Deve garantir que exista informação específica para o apoio à gestão de vulnerabilidade técnica incluindo o fornecedor de software, o número de versão, o status atual de uso e distribuição (por exemplo, que softwares estão instalados e em quais sistemas) e a(s) pessoa(s) na Empresa responsável(is) pelos softwares.

e) Deve garantir o registro e automatização das respostas as vulnerabilidades técnicas identificadas.

f) Deve garantir que na equipe de TI existam funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a análise/avaliação de riscos de vulnerabilidades, patches, acompanhamento dos ativos e qualquer coordenação de responsabilidades requerida.

g) Deve garantir que os recursos de informação a serem usados para a identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre eles sejam adequados ao negócio da Empresa e mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis forem encontrados;

h) Deve ser definido um prazo para a reação a notificações de potenciais vulnerabilidades técnicas relevantes. Esse prazo deve ser alinhado com as áreas de negócio interessadas, porém mais especificamente com as Áreas de Controles Internos, Privacidade e Jurídico;

i) Uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, deve ser avaliado os riscos associados e as ações a serem tomadas;

Tratamento de Patch e Atualizações

a) Se um patch for disponibilizado, deve ser avaliados os riscos associados à sua instalação (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação do patch);

b) Os patches devem ser testados e avaliados antes de serem instaladas para assegurar a efetividade e que não tragam efeitos que não possam ser tolerados; quando não existir a disponibilidade de um patch, convém considerar o uso de outros controles, tais como:

   i. a desativação de serviços ou potencialidades relacionadas à vulnerabilidade;

   ii. a adaptação ou agregação de controles de acesso, por exemplo firewalls nas fronteiras da rede;

   iii. o aumento do monitoramento para detectar ou prevenir ataques reais;

   iv. o aumento da conscientização sobre a vulnerabilidade;

c) Deve ser mantido um registro de auditoria de todos os procedimentos realizados;

d) Com a finalidade de assegurar a eficácia e a eficiência, deve ser monitorado e avaliado regularmente o processo de gestão de vulnerabilidades técnicas;

- **Prevenção, Detecção e Correção de Software Malicioso.**

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

a) Deve assegurar que medidas preventivas, de detecção e corretivas sejam estabelecidas corporativamente, em especial correções de segurança *(patches)* e controles de vírus, para proteger os sistemas de informação e tecnologias contra malwares (vírus, *worms, spyware, spam.)*.

- **Segurança de Rede.**

  a) Deve garantir que técnicas de segurança e procedimentos de gestão relacionados (como *firewalls*, aplicativos de segurança, segmentação de rede e detecção de intrusão) sejam utilizados para autorizar o acesso e controlar os fluxos de informação entre redes.

- **Comunicação de Dados Confidenciais.**

  a) Deve assegurar que as transações de comunicação de dados confidenciais ocorram somente por um caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovante de envio, comprovante de recebimento e não-rejeição de origem.

- **Teste de Segurança, Vigilância e Monitoramento.**

  a) Deve garantir que a implementação de segurança de TI seja testada e monitorada proativamente.

  b) Deve garantir que atualização do inventário dos ativos de TI seja realizada de forma automatizada e regular.

  c) A segurança de TI deve ser revalidada periodicamente para garantir que o nível de segurança aprovado seja mantido.

5.6. CONTROLES COMPENSATÓRIOS

a) Em situações em que a regra ou procedimento padrão não for possível ser aplicada sem prejuízo ao negócio, deverá ser declarado um Controle Compensatório. Controles compensatórios são um conjunto de medidas ou ações tomadas para compensar uma mudança ou variação em um processo ou sistema, com o objetivo de manter uma determinada condição ou nível de desempenho.

b) O objetivo desse documento é esclarecer a Empresa que, embora o risco exista, um Gerente Corporativo compreende a relevância da questão e providenciou um meio compensatório para proteger os interesses da Empresa.

c) O documento gerado deverá ser registrado no sistema de gestão de serviços de TI da Empresa.

d) Anualmente, a Área de TI deverá realizar uma revisão em todos os riscos e controles compensatórios registrados e mitigar os riscos ou gerar uma nova versão do Controle Compensatório.

e) O artefato para registrar o Controle Compensatório deve ter o seguinte conjunto de dados:

   i. Identificação dos atores:

      1. Usuário do sistema ou processo;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

2. Gestor imediato;
3. Gerente Corporativo.

ii. Matriz de risco com os seguintes dados:

1. Descrição do Risco;
2. Área de Negócio impactada;
3. Processo de Negócio envolvido;
4. Grau de risco (Muito Alto, Alto, Médio, Baixo, Muito Baixo).

iii. Mitigação do Risco

1. Nome do Controle Compensatório;
2. Descrição do procedimento de mitigação do Risco.

5.7. ATIVIDADES REGULARES DA SEGURANÇA DA INFORMAÇÃO (SI)

As rotinas da área de TI relativas a SI corresponde a um conjunto de atividades regulares que atendem aos aspectos da gestão de SI na Empresa. Em geral, essas atividades consomem a maior parte do tempo da equipe de Segurança da Informação. Tais atividades podem ser observadas abaixo:

- Definir e manter um plano de segurança de TI e Privacidade de Dados;
- Definir, implementar e operar um processo de gestão de identidades (contas);
- Monitorar incidentes de segurança reais e potenciais;
- Revisar e validar periodicamente os privilégios e direitos de acesso de usuários;
- Implementar e manter procedimentos para manter e proteger chaves criptográficas;
- Implementar e manter controles técnicos e procedimentais para proteger a comunicação de dados através das redes;
- Conduzir frequentemente análise de vulnerabilidades no ambiente de TI.

5.8. METAS E MÉTRICAS PARA A OPERAÇÃO DOS SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO

As seguintes metas devem ser observadas relativo ao controle de revisão de acesso:

a) Assegurar que informações confidenciais e críticas são protegidas daqueles que não deveriam ter acesso às mesmas.

b) Identificação, monitoração e reporte de vulnerabilidades e incidentes de segurança;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

c) Detecção e solução de acessos não autorizados às informações, aplicações e infraestrutura;

d) Minimização do impacto de vulnerabilidades e incidentes de segurança.

Como métricas devem ser observadas as seguintes:

a) Quantidade e tipo de suspeitas e casos reais de violação de acesso;

b) Percentual de usuários que não estão em conformidade com os padrões de senhas;

c) Quantidade e tipo de códigos maliciosos prevenidos.

Anualmente, um relatório com esses dados deverá ser gerado pela área de TI.

5.9. REFERÊNCIAS

Os usuários dos sistemas da informação da Empresa devem anuir, no mínimo, com as responsabilidades desse conjunto de Políticas e Procedimentos:

a) PL – Política de Segurança da Informação;
b) PL – Política de Recursos de TI;
c) PL – Política de Privacidade de Dados;
d) PL – Propriedade Intelectual
e) PC – Descarte de equipamentos e informações
f) PC - Revisão de acesso
g) PC - E-mail e mensagens eletrônicas
h) PC - Segregação de Funções em Sistemas da Informação
i) SITE: http://marceloegito.wordpress.com (acessado em agosto 2024)
j) ABNT NBR ISO_IEC_20000
k) ABNT NBR ISO_IEC_27000
l) ITGI / ISACA - COBIT 5
m) ITILV3_Glossary_Brazilian_Portuguese_v3.1.24.pd
n) ITIL - ITIL Service Management – Service Design
o) ITIL - ITIL Service Management – Service Transition
p) ITIL - ITIL Service Management – Service Operation

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

6. POLÍTICA DE CONTROLE DE ACESSO

6.1. OBJETIVO

Este documento tem como objetivo definir o processo de concessão, gerenciamento de contas de usuários e respectivos perfis para acesso aos sistemas de informação da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

6.2. APLICAÇÃO

Quaisquer processos de disponibilização, gestão ou revogação de acessos gerenciados pela área de Tecnologia da Informação da ENGECOMP.

6.3. RESPONSABILIDADES

TI - Segurança da Informação.

- Definir o processo de concessão, gerenciamento e cancelamento de contas de usuários e respectivos perfis de acesso aos sistemas de informação.
- Conduzir anualmente a análise crítica dos direitos de acesso dos usuários.

Recursos Humanos.

- Notificar formalmente o Administrador de Segurança sobre atestados ou afastamentos, tais como, mas não se limitando a: afastamento por doença (ocupacional ou auxílio acidente), transferências temporárias, licença maternidade etc.
- Fornecer regularmente (em base diária se necessário) a lista dos usuários demitidos.

Clientes e Parceiros.

- Devem informar à ENGECOMP sobre atestados ou afastamentos e demissão de usuários cadastrados pela ENGECOMP em seus próprios sistemas para que os Administradores de Segurança da ENGECOMP possam tomar as ações apropriadas (remoção ou bloqueio de direitos de acesso).

6.4. ACESSO A SISTEMAS

a) Antes de liberar os sistemas da ENGECOMP em ambiente de produção, a Área de TI (Segurança da Informação) deverá certificar-se que há evidência de que o sistema de gerenciamento de segurança atende aos padrões providos pela ENGECOMP.
b) Terceiros devem concordar por escrito em manter o gerenciamento de Segurança da Informação de acordo com os padrões da ENGECOMP até o final do contrato.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

c) Todos os usuários devem ser autenticados e autorizados antes que recebam acesso às informações e sistemas da ENGECOMP.
d) Antes de obter acesso aos sistemas de informação da ENGECOMP, os Colaboradores devem assinar o TERMO DE RESPONSABILIDADE PARA USO DE RECURSO CORPORATIVO DE TECNOLOGIA DA INFORMAÇÃO.
e) As credenciais fornecidas a terceiros, prestadores de serviço ou parceiros comerciais possuirão data de expiração máxima de 90 dias, podendo ser prorrogado em caso de contratos com prazo de vigência superior a referidos 90 dias, por um período máximo de até 180 dias.
f) As solicitações de acesso podem ser feitas para usuários individuais ou lote de usuários, terceiros ou colaboradores internos. Em caso de solicitação em lote, todos os procedimentos de validação da legitimidade do acesso, da responsabilização dos usuários e da chefia imediata, seguirão os mesmos procedimentos das solicitações individuais.
g) Todas as solicitações de acesso devem ser documentadas e somente devem ser processadas após o término do fluxo de aprovações. As solicitações devem ser arquivadas de forma que seja possível localizá-las prontamente quando necessário.
h) O usuário deve obter aprovação do Gestor da Informação de suas aplicações e/ou informações.
i) Um Diretor ou Gerente pode delegar a função de aprovador a um subordinado, desde que este seja no mínimo contratado como Coordenador, ficando responsável por ele.
j) Um Coordenador não pode delegar a função de aprovador.
k) As credenciais de usuário devem ser claramente associadas ao Colaborador responsável pelo mesmo, não sendo permitido que as credenciais sejam genéricas, descritivos ou anônimos. Os casos onde a criação de uma credencial genérica seja comprovadamente necessária, deverão ser analisados individualmente pela Área de TI (Segurança da Informação) e aprovado pela diretoria de TI.
l) A criação, exclusão ou manutenção de usuários e grupos de usuários, bem como a atribuição de permissões em diretórios deve ser efetuada somente pelos colaboradores devidamente designados pelo gestor da área de Sustentação.
m) A concessão de acessos deve ser efetuada através do uso de perfis de acesso pré-definidos. A definição dos perfis de acesso deve levar em consideração os requisitos de segurança e a necessidade de negócio dos usuários de acessar a informação.
n) É responsabilidade do Colaborador requerente e do gestor aprovador, zelar pela veracidade das informações providas no formulário de solicitação de acesso.
o) É proibido tentar acessar recursos adicionais aos que foram atribuídos ao Colaborador pelo seu gestor imediato. Qualquer acesso não autorizado será considerado falta grave.

6.5. PROCEDIMENTOS DE CONTROLE DE ACESSO DOS SISTEMAS

a) Acessos privilegiados aos sistemas de produção devem ser limitados a pessoas que comprovadamente necessitem deste acesso para execução do seu trabalho ou resolução de problemas emergenciais.
b) A equipe de Desenvolvimento de Aplicação não deve receber privilégios para atualizar sistemas ou acessar dados de produção, exceto para resolução de problemas quando e previamente autorizado pelo gestor.
c) Os colaboradores da área de TI não devem receber privilégios para modificar softwares de sistema, softwares de aplicação e informações de produção sem que haja um documento de mudança previamente aprovado pelo Comitê de Segurança da Informação.
d) As contas usadas por fornecedores/prestadores de serviço para manutenção remota devem ser habilitadas somente durante o tempo necessário para a execução da manutenção.
e) Deve haver uma documentação consistente de todos os usuários de sistemas em rede e seus perfis de acesso.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

f) A equipe de Suporte Técnico irá realizar o fluxo de validação do acesso dos programas com o seguinte esquema:
- Usuário ou o gestor do usuário: solicita e justifica o acesso;
- Gestor do usuário (supervisor ou coordenador): avalia e aprova a necessidade, podendo ser concedido acesso individual ou em lote;
- Gestor do grupo (gerente ou diretor): confirma o privilégio de acesso e compreende os riscos envolvidos, caso existam;
- Gestor do modulo / rotina ou programa (gestor da informação): é informado sobre o acesso e pode revogar a autorização do Gestor do grupo apontando os riscos válidos;
- Líder da subcomissão de Segurança ou delegado do Diretor de TI: avalia os riscos dos acessos e pode revogar a autorização do Gestor do Grupo conforme apontamento dos riscos.

g) Todas as solicitações de acesso que não envolvam perfis pré-definidos devem ser avaliadas e aprovadas pela Área de TI (Segurança da Informação). É obrigatório manter um histórico dessas solicitações.
h) A Área de TI (Segurança da Informação) deve conduzir regularmente (ao menos um por ano ou conforme demandas acordadas com as áreas de negócio) a análise crítica dos direitos de acesso dos usuários.
i) A Área de TI (Segurança da Informação) deve aplicar a Política de Inatividade sobre a data do último acesso.
j) O departamento de Recursos Humanos deve fornecer uma lista dos usuários demitidos para que o Administrador de Segurança possa tomar as ações apropriadas (remoção ou bloqueio de direitos de acesso).
k) Clientes e Parceiros devem informar prontamente à ENGECOMP ou suas empresas controladas e subsidiária integral atestados ou afastamentos e demissão de colaboradores cadastrados pela ENGECOMP em seus próprios sistemas para que a área de Tecnologia da Informação possa tomar as ações apropriadas (remoção imediata ou bloqueio de direitos de acesso).
l) Nos processos de exclusão de contas de usuários demitidos, deve-se atentar para os acessos a equipamentos, sistemas ou quaisquer recursos de tecnologia utilizados para processar, armazenar ou transportar informações, que requeiram autenticação.
m) Não é permitido o acesso de visitantes à rede e outros recursos tecnológicos a menos que justificado e autorizado formalmente.
n) A Área de TI (Segurança da Informação) da ENGECOMP reserva-se no direito de monitorar e auditar a utilização dos recursos corporativos concedidos ao usuário. Pode ainda suspender temporariamente o acesso em caso de suspeita de uso inadequado, notificando os seus responsáveis.
o) Quaisquer acessos com privilégio elevado (administrador) para Sistemas, Rede ou Banco de Dados deve ser aprovado, além do gestor do Requisitante, pelo responsável por Segurança da Informação e Diretoria de TI
p) Qualquer perfil criado sem a aprovação necessária será revogado pela Área de TI (Segurança da Informação) sem aviso prévio.

6.6. BLOQUEIO E REVOGAÇÃO DE ACESSO

a) Deve-se bloquear toda Conta de usuário que estiver sem uso por mais de 35 dias.
b) A análise de acessos com vistas a revogação dos privilégios de uso, depende de registro mínimo de ao menos 45 dias de atividade. Caso for constatado que nesse período um determinado modulo, rotina ou programa, ficou sem acesso, o referido privilégio de acesso será revogado.
c) Colaboradores demitidos, independentemente do perfil de acesso que possuam, devem ter seus acessos bloqueados em até 01 (dia). A Área de TI (Segurança da Informação) fará auditorias para verificação da efetivação do bloqueio após a situação do colaborador ser refletida na base da área de Recursos Humanos (RH) ou após notificação do gestor imediato, prevalecendo a data na base do RH.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

d) Devem ser removidos os privilégios das Contas de Acesso imediatamente após a comunicação da necessidade do bloqueio ou no caso de sindicância pela Área de TI (Segurança da Informação).
e) A solicitação de bloqueio para os prestadores de serviços deve ser realizada pelo Gestor do contrato de prestação de serviços, imediatamente após o término do contrato ou da prestação de serviços, e ainda em casos específicos de rescisão.
f) O solicitante da conta deverá informar imediatamente a área de Tecnologia da Informação através de chamado no Service Desk quando a conta e/ou privilégios concedidos não sejam mais necessários, para que eles sejam revogados.
g) A base de cadastro de Colaboradores do RH deve ser atualizada e utilizada diariamente para identificação e desativação das Contas de Acesso de Colaboradores demitidos.
h) Caso seja atribuído um novo dono para uma Conta de Serviço será necessário alterar a senha.
i) Sempre que ocorrer a alteração do colaborador entre departamentos e que o mesmo perca os direitos sob informações confidenciais e/ou sensíveis da área onde trabalho anteriormente, a Área de TI (Suporte Técnico) deve cancelar o acesso do colaborador e suspender quaisquer acessos a sistemas, sendo de obrigação do novo gestor solicitar, novamente, os acessos necessários para o colaborador movimentado devem ser providenciados pelo novo gestor.
j) O colaborador que permanecer em licença com duração superior a 180 (cento e oitenta) dias terá direito de acesso aos recursos de TI revisado conforme o regramento interno aplicado ao caso.
k) O colaborador que tiver sua relação contratual com a Empresa encerrada terá seu acesso aos recursos de TI suspenso. Dados pessoais mantidos em sistemas de armazenamento corporativo deverão ser auditados antes de liberados para no distrato. Contas de acesso serão direcionadas para o gestor da área. Após 60 (sessenta) dias do desligamento, as contas serão apagadas ou anonimizadas.
l) O prestador de serviços interno que tiver sua relação contratual com a Empresa encerrada terá seu acesso aos recursos de TI suspenso no momento da notificação do distrato. Dados pessoais mantidos em sistemas de armazenamento corporativo deverão ser auditados antes de liberados para no distrato. Contas de acesso serão direcionadas para o gestor da área. Após 60 (sessenta) dias do desligamento, as contas serão apagadas ou anonimizadas.
m) O prestador de serviço interno que estiver sem contrato ou com ele em vacância com duração superior a 90 (noventa) dias terá direito de acesso aos recursos de TI revogado conforme o regramento interno aplicado ao caso. No caso da vacância, após o período de 90 (noventa) dias, as contas serão apagadas ou anonimizadas e os dados pessoais, se existirem no OneDrive Corporativo, serão apagados.

6.7. GESTOR DA INFORMAÇÃO

a) O superior imediato de cada Colaborador da ENGECOMP deve aprovar todas as solicitações de acesso e, é a pessoa responsável por assegurar que os direitos de acesso estão de acordo com as tarefas do Colaborador.
b) O Gestor da Informação deve aprovar os direitos de acesso aos recursos de sua propriedade.
c) A Área de TI (Segurança da Informação) em conjunto com os Gestores de cada área deve avaliar anualmente os acessos concedidos à sua aplicação (revisão de perfis), autorizando ou limitando os acessos à mesma e cancelando os acessos dos usuários que não tenham mais necessidade de acessar determinadas informações.
d) As informações e papéis de trabalho utilizados no processo de revisão de perfis devem ser padronizados e arquivados pela Área de TI (Segurança da Informação).
e) Somente a Área de TI (Segurança da Informação) e a área que estiver revisando os perfis poderão ter acesso aos resultados das revisões, salvo em caso de auditoria e por solicitação do dono da informação (cliente).

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

f) Caso sejam identificados problemas durante as revisões de perfil, a Área de TI (Segurança da Informação) deverá acompanhar o status das correções dos problemas identificados junto às áreas envolvidas no processo de revisão.
g) As tarefas de rotina do Gestor podem ser delegadas, por exemplo, para um Custodiante da informação que cuide do ativo/informação no dia a dia, porém a responsabilidade pela informação permanece com o Gestor.
h) Os Gestores de informação deverão implementar controles apropriados para garantir a inexistência de conflito de interesses, conforme padrão estabelecido pela Área de TI (Segurança da Informação).
i) Onde não for possível aplicar o princípio da segregação de funções, devem ser implementados controles adicionais.
j) Sempre que houver uma mudança considerada importante nos processos ou na estrutura da organização, os Gestores da Informação devem rever a segregação de funções.

6.8. GERENCIAMENTO DE PRIVILÉGIOS E CREDENCIAIS EMERGENCIAIS

a) A Área de TI (Segurança da Informação) deve manter um registro de todos os usuários com privilégios especiais (administradores locais das máquinas).
b) Os Privilégios especiais devem ser autorizados e controlados pela Área de TI (Segurança da Informação) e devem ser estritamente limitados aos Colaboradores que necessitam de tais privilégios para propósitos específicos do negócio da ENGECOMP.
c) Os Administradores de sistema devem possuir usuários comuns para executar suas tarefas operacionais diárias.

6.9. COMUNICAÇÃO REMOTA COM A REDE

Não são permitidas conexões remotas com a rede de dados da ENGECOMP exceto em casos aprovados e liberados pelas Diretorias Executivas em linha com recomendações da Subcomissão de Segurança e Privacidade.

6.10. EXCEÇÕES

Não se aplica.

6.11. DOCUMENTOS REFERENCIADOS

a) Política de Segurança da Informação
b) Política de Segregação de Funções.
c) Termo de responsabilidade para uso de recurso corporativo de tecnologia da informação.
d) Política de Inatividade

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

7. POLÍTICA DE SEGREGAÇÃO DE FUNÇÕES

7.1. OBJETIVO

Este documento tem como objetivo regulamentar a liberação e mitigação de conflitos de segregação de funções (SoD) dentro dos sistemas de informação da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

7.2. APLICAÇÃO

Quaisquer sistemas de gerenciamento de informação gerenciados pela área de Tecnologia da Informação da ENGECOMP.

7.3. RESPONSABILIDADES

TI - Segurança da Informação.

- A área de Segurança da Informação de TI é a responsável por eliminar ou mitigar os conflitos de SoD, reconhecendo a necessidade de proteger ativos, gerenciar o acesso às informações e melhorar a qualidade dos controles das informações críticas dos negócios (ou seja, financeiras, operacionais, regulatórias, pessoais etc.).
- Manter atualizada a lista de conflitos de funções, programas ou rotinas dos sistemas da informação.
- Conduzir regularmente a análise crítica dos privilégios de acesso dos usuários.
- Gerar regularmente (ao menos um por ano ou conforme demandas acordadas com as áreas de negócio) o relatório de SoD a ser enviado para os gestores das áreas de negócio.

TI – Suporte Técnico

- Criar e manter a estrutura de perfis de acesso para os sistemas, programas ou rotinas de negócio nos sistemas da informação de acordo com seu protocolo interno.
- Alertar o superior imediato, gerente ou diretor responsável pelo usuário quando um conflito de SoD for revelado durante a atribuição inicial de privilégios de acesso ou durante as atribuições subsequentes como resultado de alterações nas responsabilidades do trabalho.
- Garantir que nenhuma combinação de transações com conflitos de SoD seja atribuída aos funcionários, a menos que seja aprovada pelo Diretor ou Proprietário da Informação apropriado.
- Garantir, com o apoio das áreas de negócio e RH a exatidão dos dados de registro e acesso dos usuários dos sistemas de informação. Dados como nome do usuário, superior imediato, *key user* do sistema, unidade de lotação e perfil de acesso (por semelhança de acesso ou função) são fundamentais.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Todos os supervisores, coordenadores, gerentes e diretores são responsáveis por:

a) Garantir que os funcionários que se reportam a eles não tenham conflitos de SoD como resultado dos privilégios de acesso a programas, rotinas ou funções atribuídas a eles.
b) Garantir que os programas, rotinas ou funções sejam removidas de um funcionário quando ele sair da empresa ou passar para uma nova posição dentro da empresa.
c) Garantir, com o auxílio da área de Recursos Humanos e Suporte Técnico a exatidão dos dados de registro nos sistemas de todos os funcionários sob sua responsabilidade.
d) Garantir, com o auxílio da área de Suporte e Segurança da Informação que acessos duplicados ou não utilizados por mais de 45 dias sejam removidos dos funcionários sob sua responsabilidade.
e) Buscar assistência ou orientação junto às Áreas de Suporte ou Segurança da Informação ou de seus controladores, conforme necessário, para garantir que os conflitos de SoD em sua unidade ou departamento sejam eliminados ou mitigados.
f) Garantir que todos os conflitos de SoD de médio e alto risco sejam eliminados ou mitigados dentro de suas organizações dentro de 30 dias após o recebimento dos relatórios de SoD da área de Segurança da Informação.
g) A partir dos relatórios regulares de SoD recebidos da Área de Segurança da Informação (ao menos um por ano ou conforme demandas acordadas com as áreas de negócio), avaliar se os funcionários com transações que causam conflitos de SoD continuam a precisar dessas transações e se há controles de mitigação adequados se essas transações precisarem continuar a ser mantidas.

7.4. CONSIDERAÇÕES GERAIS

a) A premissa fundamental da segregação de funções (SoD) é que ninguém pode controlar ou executar todos os aspectos principais de uma transação ou processo de negócio. A segregação de funções é uma atividade de controle importante que ajuda a detectar erros em tempo hábil e impede atividades impróprias.

b) Ao determinar a atribuição apropriada de funções, deve-se considerar o seguinte:

c) Ter pelo menos duas pessoas envolvidas em cada processo / subprocesso.

d) Ter duas pessoas envolvidas em determinados controles (ou seja, às vezes um único controle pode ser dividido em atividades que foram atribuídas a indivíduos diferentes, por exemplo, preparação e revisão de uma reconciliação bancária)

e) Cada sistema da informação deve ter uma pessoa designada como Gestor da informação, autorizado a definir e validar a lista de conflito de funções nos sistemas por ela administrado.

f) Esses indivíduos, chamados Proprietários da Informação, são responsáveis por se comunicar adequadamente dentro da empresa para garantir o acesso adequado ao sistema com base nas tarefas do funcionário.

g) Quando existirem conflitos de função, cada área de negócio, em linha com os Proprietários da Informação, deverá reatribuir funções e responsabilidades ou documentar os conflitos e responsabilizações apropriados para minimizar os riscos inerentes se a segregação de funções não for mantida.

h) Os conflitos SoD podem ser classificados em função do risco de comprometimento das funções organizacionais.

i) Todos os conflitos SoD de alto e médio risco criados como resultado da aplicação de funções ou rotinas dos sistemas da informação devem ser eliminados ou mitigados de acordo com as diretrizes fornecidas nesta política.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

7.5. PROCEDIMENTOS - CONTEXTO DE APLICAÇÃO

As seguintes categorias de deveres ou responsabilidades, embora não sejam abrangentes, são consideradas incompatíveis e devem ser separadas:

- Iniciar uma transação e aprovar a mesma transação.
- Atualização de registros de fornecedor / funcionário e aprovação de transações financeiras relacionadas a esse fornecedor / funcionário.
- Processar transações e conceder autorização de acesso a sistemas / aplicativos.

7.6. ELIMINANDO OU MITIGANDO CONFLITOS DE SOD

a) Os procedimentos internos de trabalho das áreas de negócio devem incluir controles projetados para prevenir e detectar fraudes ou erros inadvertidos que possam ocorrer em relação à integridade e / ou processamento de dados críticos para os negócios. Portanto, os seguintes procedimentos devem ser seguidos na atribuição de privilégios de acesso aos funcionários:

b) Quando um novo funcionário ou um funcionário existente precisar acessar rotinas, programas ou funções nos sistemas da informação para desempenhar suas responsabilidades no trabalho, o superior imediato, gerente ou diretor responsável pelo usuário solicitará o acesso à Área de TI através de registro de chamado no Service Desk.

c) A Área de TI analisará as solicitações de acesso com auxílio da lista de conflitos de funções, programas ou rotinas dos sistemas da informação fornecida pelo fabricante do sistema ou desenvolvedor. Se um conflito de SoD for identificado por meio dessa análise, os seguintes procedimentos serão seguidos para eliminar ou mitigar o SoD:

d) Se o conflito de SoD é devido a uma transação usada pelo funcionário, o superior imediato, gerente ou diretor responsável pelo usuário deve verificar se as responsabilidades do trabalho do funcionário podem ser reatribuídas para que a transação causadora de conflito de SoD possa ser removida do funcionário e o conflito possa ser eliminado.

e) Se não for possível evitar ou mitigar o conflito, o fato deverá ser documentado e aprovado pelo Diretor da área solicitante e repercutido para as diretorias afetadas.

f) Se o conflito de SoD é devido a uma transação que um funcionário não usa, o superior imediato, gerente ou diretor responsável pelo usuário deve trabalhar com a Área de TI para determinar se a transação é usada por alguém na Empresa.

g) Se a transação não estiver sendo usada por ninguém na Empresa, ela poderá ser removida ou bloqueada no sistema e, assim, eliminar o conflito de SoD.

h) Se isso não for possível, o conflito de SoD deve ser mitigado em conjunto com o controlador apropriado e a mitigação deve ser documentada e aprovada pelo dono da informação ou diretor responsável pela área de negócio envolvida com a rotina ou transação.

7.7. EXCEÇÕES À APLICAÇÃO DESSA POLÍTICA

Não se aplica.

7.8. DOCUMENTOS REFERENCIADOS

- Política de Segurança da Informação Corporativa
- Política de Controle de Acesso

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

8. POLÍTICA DE GESTÃO DE MUDANÇAS

8.1. OBJETIVO

A finalidade dessa política é controlar de forma padronizada o ciclo de vida de todas as mudanças garantindo que mudanças importantes para a organização possam ser realizadas com o menor número de interrupções dos serviços de TI e garantir que os riscos inerentes a cada mudança possam ser devidamente gerenciados e mitigados na ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

8.2. APLICAÇÃO

Quaisquer processos de disponibilização, gestão ou revogação de acessos gerenciados pela área de Tecnologia da Informação da ENGECOMP.

8.3. RESPONSABILIDADES

Responsabilidades Operacionais

- As responsabilidades operacionais estão estruturadas da seguinte forma:

Líder da Subcomissão de Mudanças, cumpre os seguintes papéis:

- Definir a estratégia dos processos da mudança.
- Dar suporte aos envolvidos em cada processo da mudança.
- Garantir que cada processo esteja de devidamente documentado e atualizado.
- Auditar periodicamente os processos, garantindo o cumprimento de padrões e políticas.
- Rever periodicamente a estratégia dos processos, garantindo que os mesmos ainda são necessários.
- Manter o processo de comunicação de informações adequado.
- Garantir recursos técnicos e de negócio necessários para os processos, apoiando as atividades necessárias durante todo o ciclo de vida gerenciamento de serviços.
- Endereçar questões relevantes para os responsáveis, garantindo o desenrolar do processo.
- Contribuir a melhoria constante do serviço prestado.

Comitê Consultivo de Mudanças (CCM) ou subcomissão de Mudanças, cumpre os seguintes papéis:

- A Comissão de Mudanças, Privacidade e Segurança tem o papel de CCM.
- Corpo consultivo que suporta a autorização de mudança e ajuda o gerenciamento de mudança na avaliação, priorização e programação da mudança.
- Autoridade de mudança para uma ou mais categorias de mudança. Categoria essa que dever ser classificada entre baixa, significante ou alta.
- Obtém autorização formal para cada mudança de uma autoridade de mudança, que pode ser: um papel, pessoa ou grupo de pessoas (Gerente de Mudanças, CCM, CCME, gestores de TI ou de negócio).

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Comitê Consultivo de Mudanças Emergencial ou CCME, cumpre os seguintes papéis:

- Corpo consultivo que deve ser consultado em casos de emergência, quando é possível convocar uma reunião de todo o CCM para a autorização de mudança.

Deve documentar qualquer decisão para autorizar uma mudança emergencial e garantir que acordo formal do gerenciamento correto tenha sido recebido e prover os registros adequados.

8.4. CONSIDERAÇÕES GERAIS

A Política de gestão de Mudanças visa aumentar da taxa de sucesso de alterações no ambiente tecnológico da organização. esse direcionamento exige suporte executivo para a implementação da cultura que vai orientar a forma como as expectativas de TI e do negócio serão atendidas.

Como resultando desse esforço, há a seguinte expectativa:

- Redução do trabalho não planejado.
- Tolerância 0 (zero) para mudanças não autorizadas.
- Incorporar o conceito gerenciamento de mudanças e roteiros da mudança.
- Controles segregados para aprovação de execução e aceite de mudanças.
- Rastreabilidade da mudança.
- Agenda de mudanças flexível para aceitar exceções.
- Avaliação de riscos e desempenho de todas as mudanças que impactam na capacidade do serviço.
- Responder às necessidades de negócio enquanto aumenta o valor e reduz incidentes, interrupções e reparo.
- Garantir que a organização registre e avalie as mudanças e priorize, planeje, teste, implemente, documente e revise de maneira organizada as mudanças autorizadas.

8.5. METAS E MÉTRICAS

O seguinte conjunto de metas e métricas serão empregados para o acompanhamento dessa política:

- Mudanças autorizadas são realizadas em tempo hábil e com o mínimo de erros, envolvendo a requisição, análise, autorização, teste, revisão e liberação:
- Quantidade de retrabalho causado por falha na mudança.
- Redução de tempo e esforço necessários para fazer mudanças.
- Número e idade das solicitações de mudança em backlog.

As avaliações de impacto revelam o efeito da mudança em todos os componentes a serem afetados (plano de riscos e roolback):

- Percentual de mudanças malsucedidas devido a avaliações de impacto inadequados.
- Todas as mudanças emergenciais são revistas e autorizadas após a mudança:
- Percentagem de mudanças no total que são soluções de emergência.
- Número de mudanças emergenciais não autorizadas após a mudança.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Os gestores de negócio e de TI são informados de todos os aspectos da mudança:

- Classificações do feedback dos gestores sobre nível de satisfação.
- Toda mudança deve ter um plano de remediação ou rollback. Um plano de remediação é definido como sendo ações a serem tomadas para recuperação após a mudança ou liberação que falhou.
- Toda mudança deve ter um plano de riscos. O plano de riscos deve seguir as políticas e procedimentos declarados no processo de gestão de riscos de TI.
- Nenhum procedimento de mudança deve ser executado ou agendado durante os períodos de freeze, essas datas devem ser pré-estabelecidas durante o ano vigente.

8.6. CATEGORIA DAS MUDANÇAS

As mudanças devem ser:

- **Mudança padrão ou pré-autorizada**: tipo de mudança de um serviço ou infraestrutura que está pré-autorizada pelo gerenciamento de mudança e tem um procedimento definido e aceito para fornecer um requisito específico de mudança.
- **Mudança normal**: tipo de mudança que é levantada por uma requisição do iniciador (indivíduo ou grupo organizacional) que requer a mudança.
- **Mudança emergencial:** tipo de mudança que tem a intenção de reparar um erro e um serviço de TI que está causando alto impacto negativo no negócio. Quando possível, é testada antes do uso, pois o impacto da mudança emergencial pode ser maior do que aquele do incidente original.

8.7. PROCEDIMENTOS

Escopo do processo

Por definição mudança de serviço se refere a adição, modificação ou remoção de um serviço ou componente de serviço devidamente autorizado, planejado ou suportado e sua respectiva documentação. Sendo assim, esta política se aplica a toda e qualquer mudança de serviço, onde podemos definir serviço como um meio de entregar valor aos clientes, visando proporcionar resultados pretendidos sem a propriedade de custos e riscos específicos; sendo que esses resultados são possíveis a partir do desempenho de tarefas e são limitados pela presença de restrições a serem determinadas.

Por sua vez os serviços são constituídos por processos, pessoas, infraestrutura, sistemas e informações; estes, portanto, são o alvo em última instância do propósito desse processo.

Produtos de trabalho

Entradas:

- Políticas e estratégias de mudança e liberação.
- Formulário de Requisição de Mudança.
- Planos de mudança, liberação, implementação, teste, avaliação e remediação.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Cronograma de mudança.
- Resultados dos testes, relatório de teste e relatório de avaliação.

Saídas:

- Relatório de Requisição de Mudanças rejeitadas
- Relatório de Requisição de Mudanças aprovados
- Planos de mudança autorizados
- Mudança de documentos e registos
- Relatórios da Gestão da Mudança.

Em linha com o mapa do processo, os procedimentos básicos para a gerenciamento das mudanças são os seguintes:

O QUE	QUEM
Identificação da necessidade para a mudança.	Requisitante
Formalização do pedido de mudança	Requisitante
Avaliação da necessidade e dos riscos	Comitê de Mudanças
Autorização ou rejeição da execução	Comitê de Mudanças
Planejamento executivo para a realização do trabalho	Requisitante / TI
Validação do plano de trabalho	Comitê de Mudanças
Planejamento operacional para a realização do trabalho	TI
Execução	TI
Testes	Requisitante / TI
Validação dos resultados	Requisitante
Liberação para uso	TI
Documentação	TI
Encerramento	Requisitante

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Controle de risco

Para garantir o devido controle dos níveis de risco o Comitê de Controle de Mudanças (CCM) deverá ser envolvido em todas as discussões de mudanças significativas para o negócio. Entende-se por mudanças significativas aquelas que possam gerar impacto na qualidade, orçamento e prazos definidos no planejamento anual da organização. Como exemplo, mas não se limitando a isso, temos:

- Mudança de escopo de contratos existentes.
- Investimentos não planejados no orçamento em curso.
- Alteração de resultados esperados no nível da organização.

8.8. EXCEÇÕES

- Não se aplica.

8.9. DOCUMENTOS REFERENCIADOS

- Política de Segurança da Informação

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

9. POLÍTICA BACKUP

9.1. OBJETIVO

A presente política visa estabelecer na ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente "Empresa", a obrigatoriedade de:

- Registro da rotina de backup efetuada para os servidores de dados e sistemas da ENGECOMP, de acordo com o sistema operacional utilizado.
- Manter cópia segura dos dados e sistemas essenciais para proteger os processos comerciais e permitir a recuperação deles em caso de desastre.
- Assegurar que os sistemas e base de dados da ENGECOMP estão adequados às estratégias e objetivos corporativos e são corretamente mantidos e operados.
- Assegurar que somente funcionários de TI, treinados, competentes e autorizados poderão administrar os sistemas e base de dados da ENGECOMP.

9.2. APLICAÇÃO

a) Esta política se aplica a todos os sistemas de informação e base de dados da ENGECOMP que já estão em uso e que possam ser adquiridos no futuro.
b) Todos os papeis e atores na empresa estão sujeitos a essas determinações.

9.3. CONSIDERAÇÕES GERAIS

Todas as transações realizadas pela Empresa devem:

a) Estar de acordo com a legislação pertinente vigente;
b) Respeitar os princípios de Ética da ENGECOMP, bem como dos profissionais e sociedades com as quais a Empresa se relacione;
c) Obedecer aos requisitos e/ou níveis de aprovação constantes nas políticas e documentos regulatórios da Empresa.

Backup é definido como a cópia de dados de um dispositivo de armazenamento para que possam ser restaurados em caso de perda dos dados originais, alteração indevida ou até mesmo corrupção dos dados.

Compete à Área de TI manter o backup atualizado de todos os arquivos e bancos de dados da Empresa armazenados nos servidores da ENGECOMP.

Para todo e qualquer dado e/ou sistema que seja relevante para o funcionamento do negócio da ENGECOMP, a área de TI deverá assegurar que as políticas e procedimentos estabelecidos serão seguidos consistentemente.

Os backups devem ser gerados em dias úteis.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

9.4. PROCEDIMENTOS

LOG´S DE BACKUPS. Os sistemas responsáveis pelos backups completos e automáticos dos servidores geram diariamente logs, relatando informações sobre os backups efetuados. O analista de rede verifica esses logs e, em caso de falhas, existindo viabilidade, a rotina é reprogramada manualmente para a gravação dos principais arquivos durante o horário do expediente.

SISTEMA DE RODÍZIO. O sistema de rodízio garante backups completos e regulares das informações armazenadas nos servidores.

SERVIDORES A SEREM EFETUADOS OS BACKUPS. Para cada servidor a ser protegido deve-se montar uma tabela de execução de backups que identifica:

- o método empregado
- a partição ou disco a ser protegido
- a agenda do trabalho
- O modo de uso e rodízio de unidades m[oveis

RESTAURAÇÃO DE ARQUIVOS. O colaborador interessado deve solicitar a equipe de TI a restauração do arquivo de interesse com a devida aprovação do superior imediato. O responsável de TI pode rejeitar a solicitação no caso do procedimento oferecer riscos para o negócio.

TESTES DE RECUPERAÇÃO. Testes de recuperação de dados armazenados deverão ser realizados mensalmente e sua execução deverá ser registrada.

PREMISSAS. A seguinte premissa foi estabelecida para Backup de Sistemas e Base de Dados:

A rotina de Backup deve estar clara no procedimento correspondente e aprovada pela Diretor de TI.

9.5. EXCEÇÕES

Não se aplica.

9.6. DOCUMENTOS REFERENCIADOS

Política de Segurança da Informação

9.7. ANEXOS

Não se aplica.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

10. POLÍTICA DE RELACIONAMENTO COM FORNECEDORES

10.1. OBJETIVO

Definir critérios e diretrizes para orientar as atividades decorrentes do relacionamento entre a ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente "Empresa" e seus Fornecedores.

10.2. ASPECTOS GERAIS

Toda relação de funcionários da empresa com Fornecedores deve ser realizada de forma ética e profissional, em conformidade com o código de ética da empresa, mantendo-se os níveis adequados de exigência, transparência e zelo com relação aos critérios estabelecidos pela empresa.

10.3. RELACIONAMENTO EMPRESA X FORNECEDORES

Todos os Fornecedores devem ser tratados igualmente, sem preferência durante as etapas do processo de negociação e contratação de Materiais, Bens ou Serviços, que deve ser sempre conduzido pela ou sob a coordenação da da Diretoria Executiva.

Somente os funcionários da Área de Contratação e os citados na alínea "i" acima, estão autorizados a solicitar propostas comerciais e negociar com Fornecedores;

Todas as negociações de caráter técnico podem contar com a participação da Área Requisitante, cabendo a negociação comercial ser efetuada, exclusivamente, pela Diretoria Executiva e, invariavelmente, nas instalações da ENGECOMP;

A Diretoria Executiva deve ser convidada a participar de qualquer reunião com o Fornecedor que tenha como objetivo desenvolver projetos para futuras contratações, cabendo exclusivamente ela decidir quanto a sua participação;

Todas as informações compartilhadas entre a ENGECOMP e seus Fornecedores devem ser consideradas como confidenciais. Portanto, não devem ser reveladas ou utilizadas para uso diferente do estabelecido nos respectivos Contratos;

O relacionamento comercial com os Fornecedores deve ser estabelecido com base em sua qualificação e competência, sem favoritismo ou tendência, devendo ser considerado na escolha, entre outros fatores objetivos, o valor, a qualidade, o prazo de entrega e o custo dos produtos e serviços oferecidos;

O único documento reconhecido pela empresa que caracteriza a formalização de uma negociação e seu posterior pagamento é o Contrato/Pedido devidamente autorizado pela Diretoria Executiva ou nos casos especiais de alçadas deslocadas, conforme aliena "i" deste item;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

É vetada a Área de Contratação a emissão de pedidos de compra com a finalidade de regularização de pagamentos a Fornecedores, exceto quando autorizados pelo Diretor Executivo da ENGECOMP. Nestes casos a Área Requisitante é responsável por obter as aprovações necessárias em caráter excepcional;

Nenhum funcionário da ENGECOMP tem autorização para solicitar que um Fornecedor inicie a instalação de qualquer equipamento, entrega de materiais, bens ou serviços a ENGECOMP, sem estar de posse do respectivo Contrato/Pedido devidamente autorizado, liberado e assinado, por aqueles que possuem poderes para tanto, exceto quando autorizado formalmente pelo Diretor Executivo;

Todos os Pedidos de Compras somente devem ser autorizados após o recebimento do Contrato formal devidamente assinado entre as partes envolvidas com poderes formais para tal ato;

Todo convite realizado por Fornecedores para participação em seminários, eventos técnicos, cursos, visitas técnicas a escritórios, independentemente da finalidade, deverá ser encaminhado para a Diretoria de Recursos Humanos para avaliação. Caso a avaliação não seja positiva, a demanda deve ser submetida a aprovação dos Gestores responsáveis diretamente subordinados ao Diretor Executivo;

Toda e qualquer publicação ou anúncio público relativo à aquisição de Materiais, Bens e Serviços para a ENGECOMP via pregões eletrônicos, licitações, tomadas de preço, emissão de RFPs (request for proposals) ou semelhantes devem ser sempre e previamente aprovados pela Diretoria Executiva.

10.4. RELACIONAMENTO FORNECEDORES X FUNCIONÁRIOS

Todo atendimento a Fornecedores deve ser realizado com caráter igual e institucional, nunca de forma pessoal;

Todo relacionamento de funcionários da ENGECOMP com Fornecedores deve ser realizado e mantido com especial exigência e cuidado, balizado sempre na transparência e apego estrito às sistemáticas estabelecidas pela ENGECOMP;

Os funcionários da ENGECOMP devem evitar, com todos os Fornecedores, estabelecer um relacionamento, seja no âmbito pessoal ou comercial, que possa vir a caracterizar situações de Conflitos de Interesses ou afetar o julgamento imparcial e objetivo dessas eventuais situações;

Não é permitido ao funcionário da ENGECOMP participar de negociações (técnicas ou comerciais) com pessoas ligadas aos Fornecedores que possuírem qualquer grau de parentesco e/ou vínculo matrimonial. Nestes casos, o responsável superior do funcionário deve ser comunicado imediatamente e a responsabilidade de negociação deve ser transferida para outro funcionário que não se enquadre nestas hipóteses;

Se algum funcionário da ENGECOMP perceber a existência de alguma relação suspeita entre Fornecedores e funcionários da ENGECOMP, que possa ser caracterizada como Conflito de Interesses, deverá utilizar o canal de comunicação do Código de Ética, disponibilizado na Intranet da companhia, informando sobre a situação existente;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Não devem ser aceitos pelos funcionários da ENGECOMP convites para almoços, jantares, confraternizações, nem mesmo através do fornecimento de vouchers ou o recebimento de quaisquer tipos de presentes ou favores. Exceção é feita para brindes simbólicos sem valor comercial (materiais promocionais com a logomarca da empresa Fornecedora ou representante) como por exemplo, calendários, canetas, copos, blocos e semelhantes;

Sempre que um brinde recebido não atender a qualquer um dos critérios de permissão (valor simbólico, material promocional com a logomarca do Fornecedor) ou ensejar interpretações duvidosas, a situação deverá ser imediatamente submetida à Área de Contratação de Suprimentos, para análise e definição das ações a serem adotadas.

10.5. ASPECTOS FINANCEIROS E COMERCIAIS

Todas as cobranças de multa que a ENGECOMP venha a **sofrer** referente a qualquer situação contratual com Fornecedores, só poderão ter seu pagamento realizado mediante parecer prévio e favorável da Diretoria Executiva Corporativa e o “de acordo” do Diretor Executivo, salvo em casos excepcionais definidos e autorizados pela Presidência. Os valores destas multas deverão ser alocados no Centro de Custo da área requisitante do serviço;

Caberá ao Requisitante (Gestor do Contrato) responsável pelo serviço, providenciar a emissão da “Folha de Registro” no SISTEMA, no mês da realização do serviço, que expressa: o aceite, o registro na contabilidade, a aprovação e a autorização do pagamento. A ausência da "Folha de Registro" impossibilita a Gerência de Contas a Pagar de lançar a nota fiscal no SISTEMA;

Todos os pagamentos devem ser feitos em conformidade com as condições contratualmente estabelecidas, desde que as notas fiscais sejam entregues à Gerência de Contas a Pagar até a data estabelecida no “Calendário de Pagamentos a Fornecedores do ENGECOMP" e satisfaçam as condições estabelecidas;

Na hipótese de haver necessidade de antecipação do cronograma físico por solicitação da ENGECOMP, o pagamento da respectiva parcela poderá ser antecipado e efetuado em conformidade com as sistemáticas vigentes. Todavia, caso a solicitação de antecipação ocorra por requerimento do Fornecedor, o pagamento da respectiva parcela poderá, a critério exclusivo da ENGECOMP, ser antecipado, inclusive com a aplicação de desconto financeiro a ser calculado com base nas taxas praticadas à época no mercado e acertado com o Fornecedor. Em não havendo concordância desta solicitação pela ENGECOMP, o pagamento será efetuado conforme originalmente previsto no Pedido.

10.6. EXCEÇÕES

Não se aplica.

10.7. REFERÊNCIAS

- Código de Ética de ENGECOMP
- Quaisquer normas de suprimentos / compras

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

11. POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E COOKIES

11.1. OBJETIVO

Trata-se das diretrizes adotadas pela ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”, em relação à recepção, armazenamento e utilização das informações pessoais disponibilizadas pelos clientes e visitantes, para acesso e uso dos nossos serviços (sites institucionais e de serviços da ENGECOMP, denominados "serviços"), que necessitam de identificação.

11.2. TERMOS E CONDIÇÕES

Para fins desta política, a referência à empresa ENGECOMP está sendo feita como ENGECOMP.

Todos os termos e condições constantes na presente Política de Privacidade poderão ser modificados a qualquer momento pela ENGECOMP, em virtude de alterações na legislação ou nos serviços, em decorrência da utilização de novas ferramentas tecnológicas ou, ainda, sempre que, a exclusivo critério da empresa, tais alterações se façam necessárias. Diante do exposto, recomendamos aos nossos usuários que, previamente à utilização dos serviços disponíveis, seja verificada a Política de Privacidade então vigente. A utilização dos serviços disponibilizados pela ENGECOMP por qualquer usuário implicará em expressa aceitação quanto aos termos e condições da Política de Privacidade vigente na data de sua utilização. Recomendamos aqueles usuários, que não concordem com a Política de Privacidade vigente, a não utilização dos serviços da empresa, visto que a sua não aceitação por parte do cliente ou ainda, a não disponibilização das informações solicitadas, pode impedir a prestação de tais serviços.

Ressaltamos que novos serviços online, disponibilizadas pela empresa, estarão automaticamente sujeitos à Política de Privacidade vigente à época de sua utilização.

11.3. CONCEITUAÇÃO – TRATAMENTO DE INFORMAÇÕES PESSOAIS

Para o fornecimento dos serviços online aos seus clientes, a empresa adota recursos avançados visando a proteção das informações pessoais dos usuários e de seus serviços. As informações de caráter pessoal dos usuários dos serviços da ENGECOMP, entendendo-se por informações pessoais o nome completo do usuário ou razão social, endereço físico e eletrônico, número de telefone, RG, CPF ou CNPJ, número de cartão de crédito, situação financeira, patrimonial, contrato social, balanço patrimonial, preferências e padrões de acesso ("informações pessoais") não são divulgadas pela empresa, exceto nas hipóteses expressamente mencionadas neste documento.

Tais informações são coletadas por meio dos canais de atendimento e armazenadas, utilizando-se rígidos padrões de sigilo e integridade, bem como controles de acesso físico e lógico, observando-se sempre os mais elevados princípios éticos e legais.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Caso o usuário decida fornecer suas informações pessoais, tal ato implicará em expressa autorização para que tais informações sejam utilizadas para o fornecimento dos serviços, com o propósito definido em contrato de prestação de serviços, bem como para que tais informações sejam arquivadas.

Uma vez provido das informações pessoais a respeito do usuário, a empresa poderá utilizar os dados do usuário para o fim de enviar publicidade, direcionada por e-mail ou por quaisquer outros meios de comunicação, contendo informações sobre a empresa, seus produtos e serviços.

Entretanto, fica reservado ao usuário o direito de, a qualquer momento, inclusive no ato da disponibilização das informações pessoais, informar a empresa, por meio dos canais de comunicação disponíveis para o cadastramento de tais informações, do não interesse em receber tais anúncios, inclusive por e-mail, hipótese em que a empresa interromperá tais serviços no menor tempo possível.

Para que as atividades de tratamento de dados pessoais ocorram da maneira correta e nos termos pretendidos pela ENGECOMP os colaboradores e terceiros envolvidos no tratamento de dados pessoais devem:

- Tratar somente os dados necessários para o cumprimento da finalidade pretendida.
- Garantir o cumprimento dos direitos dos titulares.
- Ser transparente sobre suas atividades de tratamento de dados pessoais para com os titulares dos dados.
- Tratar os dados com ética e respeito ao titular, sem fins discriminatórios ou ilícitos.
- Implementar medidas necessárias para a garantir a segurança dos dados pessoais.
- Consultar ou o encarregado ou o comitê de privacidade em caso de dúvidas sobre o tratamento de dados.
- Reportar ao encarregado de proteção de dados qualquer suspeita de violação de dados pessoais.
- Coletar, utilizar, armazenar, compartilhar e descartar dados pessoais de acordo com nossas políticas e procedimentos.

11.4. FINALIDADE DO TRATAMENTO DOS DADOS PESSOAIS E SENSÍVEIS

Finalidades para as quais a ENGECOMP pode tratar os dados pessoais:

a) o fornecimento dos serviços, com o propósito definido em contrato de prestação de serviços assinado ou de procedimentos preliminares relacionados a um contrato, bem como para que tais informações sejam arquivadas;
b) para monitorar, adaptar, atualizar, proteger e melhorar os serviços que oferecemos;
c) para verificar a identidade do titular e garantir a segurança dos seus Dados Pessoais no sentido de assegurar a sua correta identificação;
d) para responder aos seus pedidos e necessidades de apoio;
e) para entender a forma como as pessoas utilizam coletivamente os recursos de um Site, Aplicativo ou Dispositivo (ou veículo associado);
f) para administrar conteúdo, promoções, questionários ou outros recursos de um Site, Aplicativo ou Dispositivo;
g) para lhe enviar comunicações sobre a administração das suas contas e das funcionalidades de um Site, Aplicativo ou Dispositivo;
h) para o informar sobre alterações de um Site, Aplicativo ou Dispositivo;
i) para realizar análises de tendências e análise financeira para a execução de um contrato ou contrato futuro;
j) para dar efeito aos seus direitos legais e aos seus direitos no âmbito da presente Política;

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

k) para proteção contra fraude, roubo de identidade e outras atividades ilegais no cumprimento da relação estabelecida, seja no âmbito comercial ou já contratual;
l) para estabelecer ou exercer os direitos legais da ENGECOMP ou defender reivindicações legais;
m) para cumprir as Leis Aplicáveis e as nossas outras políticas aplicáveis.

11.5. COMPARTILHAMENTO DAS INFORMAÇÕES CONFIDENCIAIS

O acesso às informações pessoais coletadas e armazenadas pela ENGECOMP é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas. É exigido, também, de toda organização ou indivíduo contratado para a prestação de serviços de apoio, que sejam cumpridas as Políticas de Segurança da Informação e o Código de Ética adotado pela ENGECOMP.

A ENGECOMP poderá revelar as informações pessoais que tenha recebido, concordando, desde já, o usuário com tal revelação, nas seguintes hipóteses:

- sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- aos seus parceiros comerciais e/ou prestadores de serviço, a fim de atender à solicitação de serviços efetuada pelos usuários;
- aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pelo banco a defender seus direitos e créditos;
- aos órgãos que administrem cadastros de consumidores;
- aos seus controladores, às empresas por ele controladas, as empresas a ele coligadas ou por qualquer forma associadas, no Brasil ou no exterior;
- para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar esta autorização.

A participação da empresa no processo é revisar as informações, valores e informativos e enviar para o usuário, um comunicado de qualquer discrepância nas informações fornecidas.

11.6. PROTEÇÃO DOS DADOS PESSOAIS

Para que as atividades de tratamento de dados pessoais ocorram da maneira correta, nos termos pretendidos pela ENGECOMP e conforme a Lei de Proteção de Dados Pessoais, os colaboradores e terceiros envolvidos no tratamento de dados pessoais devem:

- Tratar somente os dados necessários para o cumprimento da finalidade pretendida.
- Garantir o cumprimento dos direitos dos titulares.
- Ser transparente sobre suas atividades de tratamento de dados pessoais para com os titulares dos dados.
- Tratar os dados com ética e respeito ao titular, sem fins discriminatórios ou ilícitos.
- Implementar práticas adequadas de tratamento de dados e medidas de segurança técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais e proteger contra acesso não autorizado, alteração, divulgação ou destruição.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Consultar ou o encarregado ou o comitê de privacidade em caso de dúvidas sobre o tratamento de dados.
- Reportar ao encarregado de proteção de dados qualquer suspeita de violação de dados pessoais.
- Coletar, utilizar, armazenar, compartilhar e descartar dados pessoais de acordo com nossas políticas e procedimentos.

A Internet não é, por si só, um ambiente seguro e não podemos fornecer uma garantia absoluta de que os seus Dados Pessoais transferidos pela Internet estarão sempre protegidos. A transmissão de Dados Pessoais pela Internet é de responsabilidade do titular, que apenas deve utilizar sistemas seguros para acessar a Sites, Aplicativos ou Dispositivos.

O Titular de dados é responsável por manter as suas credenciais de acesso a cada Site, Aplicativo e Dispositivo seguras e confidenciais. Deve alterar frequentemente as suas credenciais de acesso e deve notificar a ENGECOMP imediatamente se tomar conhecimento de qualquer utilização indevida das suas credenciais de acesso e mudá-las imediatamente.

11.7. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

A ENGECOMP, conforme finalidade definida em cada relacionamento estabelecido com o usuário e cliente, poderá utilizar instalações de tratamento de dados controlados ou operados pelos nossos prestadores de serviços terceirizados localizados em jurisdições diferentes da jurisdição em que os seus Dados Pessoais foram originalmente recolhidos.

Especificamente, o conteúdo e os recursos de um Site, aplicativo ou Dispositivo podem ser fornecidos por meio de servidores localizados fora da sua jurisdição (incluindo, entre outros, servidores localizados nos Estados Unidos).

Os Dados Pessoais podem ser transferidos e tratados utilizando esses servidores como parte da operação de um Site, aplicativo ou Dispositivo ou em associação a qualquer uma das finalidades de tratamento indicadas na presente Política, sempre em conformidade com as disposições das Leis Aplicáveis. Essas transferências são necessárias para lhe fornecer os nossos produtos e serviços de forma eficiente e eficaz.

Ao fornecer Dados Pessoais à ENGECOMP no âmbito da presente Política de Privacidade, o usuário reconhece que os seus Dados Pessoais podem ser transferidos para locais fora da sua jurisdição. Se não quiser que os seus Dados Pessoais sejam transferidos para outras jurisdições, não forneça os seus Dados Pessoais à ENGECOMP nem utilize Sites, Aplicativos ou Dispositivos.

Se transferirmos os seus Dados Pessoais para outros países, a transferência será realizada sempre respeitando essa Política, as cláusulas contratuais ajustadas entre as Partes e a LGPD.

A ENGECOMP, dentro do seu conhecimento, transferirá os dados apenas para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado e sempre de acordo com as cláusulas contratuais específicas ajustadas entre as Partes, se o caso.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

11.8. EXTENSÃO DOS EFEITOS

Os termos da Política de Privacidade aqui expostos serão aplicados exclusivamente às informações pessoais, conforme acima definido, que venham a ser disponibilizadas a ENGECOMP, pelo usuário para a utilização de seus produtos e serviços.

Por consequência, a Política de Privacidade aqui exposta não será aplicável a qualquer outro serviço que não os disponibilizados pela ENGECOMP, incluídos aqueles sites que estejam de alguma forma vinculados ao site da empresa, por meio de links ou quaisquer outros recursos tecnológicos, e, ainda, a quaisquer outros sites que, de qualquer forma, venham a ser conhecidos ou utilizados pela empresa.

Nesse sentido, alertarmos aos usuários que os referidos sites podem conter política de privacidade diversa da adotada pela ENGECOMP ou podem até mesmo não adotar qualquer política nesse sentido, não se responsabilizando, a empresa, por qualquer violação aos direitos de privacidade dos usuários que venham a ser violados pelos referidos sites.

11.9. TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

A ENGECOMP encerrará o tratamento dos seus Dados Pessoais nas seguintes hipóteses:

- quando a finalidade foi alcançada ou os dados deixaram de ser necessários conforme essa Política;
- quando o prazo necessário para o tratamento for alcançado;
- quando o usuário solicitar a exclusão dos Dados;
- por determinação da autoridade nacional de proteção de dados ou outra autoridade legalmente constituída.

O usuário tem ciência de que, mesmo após o término do tratamento de Dados, a ENGECOMP poderá manter os Dados Pessoais para as seguintes finalidades:

- cumprimento de obrigação legal ou regulatória;
- transferência à terceiros, quando o caso;
- uso anonimizado pela ENGECOMP.

11.10. DADOS DE CONTATO

Se o usuário tiver qualquer dúvida ou preocupação sobre esta Política de Privacidade, nossas práticas de coleta e uso de Dados Pessoais, ou sobre uma possível violação de Dados Pessoais ou privacidade, entre em contato com a ENGECOMP por meio do seguinte e-mail: dpo@engecomp.com.br ou diretamente o Encarregado pelos Dados Pessoais na empresa, Sr. Marcelo Silva no e-mail: marcelo.silva@engecomp.com.br

Se o usuário nos contatar, tentaremos investigar e resolver cada questão ou reclamação no prazo de 15 dias ou em qualquer outro período exigido pelas Leis Aplicáveis.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

11.11. DIREITOS AUTORAIS

A ENGECOMP assegura que as informações (textos, imagens, sons e/ou aplicativos) contidas nos seus sites estão de acordo com a legislação e normativos que regulam os direitos autorais, marcas e patentes, não sendo permitidas modificações, cópias, reproduções ou quaisquer outras formas de utilização para fins comerciais sem o consentimento prévio e expresso da empresa.

A ENGECOMP não se responsabiliza por eventuais danos e/ou problemas decorrentes da demora, interrupção ou bloqueio nas transmissões de dados ocorridos na internet.

11.12. LEI APLICÁVEL E RESOLUÇÃO DE CONFLITOS

Toda e qualquer controvérsia oriunda dos termos expostos na presente Política de Privacidade serão solucionados de acordo com a lei brasileira, sendo competente o foro da cidade de São Paulo, SP, Comarca da Capital, com exclusão de qualquer outro por mais privilegiado que seja.

Fica claro, ainda, que utilização de serviços e as ordens comandadas fora do território brasileiro, ou ainda as decorrentes de operações iniciadas no exterior podem estar sujeitas também à legislação e jurisdição das autoridades dos países onde forem comandadas ou iniciadas.

11.13. DISPOSITIVOS MÓVEIS

Para utilização do app da ENGECOMP são obrigatórios três tipos de autorizações, descritas abaixo:

1. **Localização.** Necessário para envio de pushs personalizados e funcionamento do localizador de empresas. A empresa pode usar a sua localização para prevenção a fraudes.
2. **Telefone (fazer e gerenciar chamadas telefônicas**). Necessário para identificação do dispositivo. A empresa armazena o nome do telefone e seu ID (IMEI), apenas para conseguir realizar o processo de desbloqueio para a realização de transações financeiras. Essas informações não são compartilhadas com terceiros.
3. **Acessar fotos, mídias e arquivos do seu dispositivo.** Necessário para criação dos comprovantes ao final da transação e selecionar foto na galeria para inclusão de foto de perfil. Nenhuma informação do seu celular é lida ou armazenada pela ENGECOMP.

11.14. POLÍTICA DE COOKIES

Para oferecer a melhor experiência durante a navegação em nosso site e na internet, podemos usar cookies e coletar, tratar, armazenar e/ou compartilhar - entre a ENGECOMP e outros parceiros - informações de sua navegação, para:

- garantir maior segurança durante a sua navegação;
- aperfeiçoar sua usabilidade, experiência e interatividade na utilização dos nossos portais, sites, aplicativos, e-mails e durante a sua navegação na internet;
- fazer ofertas e/ou te dar informações mais assertivas e relevantes às suas necessidades e interesses;
- buscar maior eficiência em relação à frequência e continuidade da nossa comunicação com você;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- responder suas dúvidas e solicitações;
- realizar pesquisas de comunicação e marketing de relacionamento, para melhorar nossos produtos e serviços, bem como apuração de estatísticas em geral;

A qualquer momento o usuário pode ativar em seu navegador mecanismos para informá-lo quando eles estiverem acionados ou, ainda, para impedir que sejam.

O uso de cookies, arquivos criados pelos websites que, enquanto se navega na internet, são armazenados no navegador do usuário e ajudam a personalizar seu acesso, permitindo as seguintes vantagens:

- mais segurança durante a sua navegação;
- melhor usabilidade, experiência e interatividade na utilização dos nossos canais digitais;
- recebe informações e anúncios mais assertivos e relevantes às suas necessidades e interesses;
- participa de pesquisas de comunicação e marketing de relacionamento para melhorar nossos produtos e serviços.

Os cookies são desativados por padrão e podem ser ativados através das preferências do navegador. A navegação pode se tornar limitada e algumas funcionalidades dos sites podem ficar comprometidas.

11.15. DESCRIÇÃO DOS COOKIES NO SITE DA EAÍ?!

ASP.NET SESSION ID: Serviço de sessão do ASP.NET MVC (Linguagem de desenvolvimento do site) para identificação do usuário randômica, não utilizado pela EAÍ?!, porém presente em todas as aplicações nesta linguagem.

GOOGLE ANALYTICS: Serviço de análise web fornecido pela Google, Inc. (“Google”). O Google Analytics utiliza uma forma específica de “Cookies”, ou seja, arquivos de texto, que são armazenados no seu computador e permitem a análise do seu uso do site. A informação gerada pelo Cookie acerca da sua utilização do site será transmitida e armazenada em um servidor da Google nos EUA. a EAÍ?! salienta que o Google Analytics foi ampliado no sítio eletrônico EAÍ?! para incluir o código “gat._anonymizeIp ();” a fim de garantir a gravação anônima de endereços IP (as chamadas máscaras de IP). Devido à anonimização do IP neste site, o endereço IP do USUÁRIO/USUÁRIO é abreviado pela Google dentro do território da União Europeia e do Tratado da Comunidade Econômica Europeia. Só em casos excepcionais é que o endereço IP completo será transmitido a um servidor da Google nos EUA e aí então abreviado. A Google usa esta informação em nome da EAÍ?! para analisar a utilização do USUÁRIOS do sítio eletrônico da EAÍ?!, a fim de compilar relatórios sobre atividades do site e fornecer serviços adicionais relacionados ao seu uso e uso da Internet para o operador do site. O endereço IP transmitido para o Google Analytics pelo navegador do USUÁRIO/USUÁRIO não está consolidado com outros dados da Google. O USUÁRIO/USUÁRIO poderá impedir o armazenamento de Cookies através da definição adequada do software de navegação. Além disso, poderá impedir que a Google grave e processe os dados gerados pelos Cookies e relacionados ao uso do site (incluindo endereço IP), baixando e instalando o plug-in disponível no link e informações adicionais sobre os termos de uso e proteção de dados em https://www.google.com/analytics/terms/br.html ou https://www.google.com.br/intl/pt-BR/policies/privacy/.

TWITTER PLATAFORM: Serviço de análise web do Twitter com objetivo de otimizar o compartilhamento e acesso a plataforma Twitter através do site da EAÍ?!.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

COOKIES INTERNOS DE NAVEGAÇÃO: Utilizamos cookies de sessão em nossa área restrita afim de tornar pessoal e otimizável o acesso a mesma, são cookies que guardam a preferência do usuário em relação ao modo padrão de exibição uma vez modificada.

11.16. DADOS PESSOAIS

A ENGECOMP tem como uma de suas premissas a proteção dos Dados Pessoais de todas as pessoas envolvidas na sua cadeia de atividades.

O direito à privacidade é uma prioridade e pauta todas as ações e políticas da ENGECOMP. Dentre as atividades abrangidas por esta política, poderá ocorrer o Tratamento/Processamento de Dados Pessoais, ou seja, operações realizadas com dados pessoais, tais como, a coleta, produção, utilização, acesso, distribuição, processamento, arquivamento, eliminação, entre outros.

Desta forma, qualquer Tratamento de Dados realizado deverá respeitar as disposições gerais desta Política; a Política de Privacidade da ENGECOMP e a Política de Segurança da Informação, além dos demais documentos corporativos e políticas aplicáveis ao tema.

Este texto poderá ser atualizado a qualquer momento e os Titulares de Dados, bem como qualquer outra parte interessada poderá acessar o texto atualizado nos sites oficiais ou aplicativos da ENGECOMP.

Este texto foi atualizado em 11 de novembro de 2025.

11.17. EXCEÇÕES

Não se aplica.

11.18. REFERÊNCIAS

a) Código de Ética de ENGECOMP
b) Política de Segurança da Informação da ENGECOMP
c) ISO/IEC 27701:2019
d) Proteção de dados pessoais em conformidade com a Lei Brasileira 13.709/2018

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

12. TERMOS DE USO PARA SITES E APLICATIVOS

12.1. OBJETIVO

Este documento tem por objetivo orientar o uso de todos os Sites e Aplicativos da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa” (inclusive sites e aplicativos institucionais, de produtos e serviços e internet banking) e a todos que acessam os nossos Sites e Aplicativos.

12.2. RESPONSABILIDADES DOS USUÁRIOS

Você como Usuário é responsável:

- por todas as suas ações ou omissões realizadas nos nossos Sites e Aplicativos;
- pelos conteúdos que você enviou e/ou transmitiu nos Sites e Aplicativos; e
- pela reparação de danos causados a ENGECOMP, terceiros ou outros Usuários, a partir do seu acesso e uso dos nossos Sites e Aplicativos.

Desta forma, não nos responsabilizamos pelos itens citados acima e por indisponibilidades e falhas técnicas do sistema dos Sites e Aplicativos. Considere também que conteúdos enviados e/ou transmitidos por Usuários e/ou terceiros não representam a opinião ou a visão da ENGECOMP.

12.3. DEFINIÇÕES

- Consentimento: Manifestação livre, informada e inequívoca do titular que autoriza o tratamento dos seus dados pessoais para uma finalidade específica.
- Controlador: Segundo a LGPD é quem toma decisões referentes ao tratamento dos dados pessoais.
- Cookies: São pequenos arquivos de texto que contêm dados gerados quando o usuário navega em um website. Estes são instalados no seu navegador de internet.
- Dado Pessoal Sensível: Categoria especial de dados pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos à pessoa natural.
- Dados Pessoais: Informação relacionada a uma pessoa natural identificada ou identificável (ex.: nome, e-mail, CPF).
- Direitos dos Titulares: Explicitação dos direitos garantidos pela LGPD, como confirmação de tratamento, acesso, correção, anonimização, bloqueio, eliminação, portabilidade e oposição.
- Encarregado pela Privacidade de Dados (DPO): pessoa indicada por nós para ser o responsável por garantir o atendimento aos seus direitos e esclarecer dúvidas sobre o tratamento de seus dados pessoais.
- Finalidade: Motivo pelo qual os dados são coletados e tratados, explicitado ao titular (ex.: cadastro, envio de campanhas, cumprimento legal).
- Livre Acesso: Direito do titular de acessar, corrigir, excluir ou solicitar portabilidade de seus dados pessoais.
- Necessidade: Limitar o tratamento ao mínimo necessário para atingir a finalidade proposta.
- Operador: É a PARTE que realiza o tratamento de dados em nome do controlador.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Prestadores de Serviços: São todos os prestadores de serviços da ENGECOMP.
- Revogação de Consentimento: Direito de o titular retirar o consentimento dado a qualquer momento e conhecer as consequências dessa revogação.
- Segurança: Medidas técnicas e administrativas para proteger dados contra vazamentos, acessos não autorizados e incidentes de segurança.
- Terceiro: São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais e fornecedores com quem a ENGECOMP compartilha dados pessoais.
- Titular dos Dados: A pessoa física a quem pertencem os dados pessoais coletados que são tratados pela ENGECOMP.
- Transparência: Garantia de informações claras e acessíveis sobre o tratamento dos dados e seus responsáveis.
- Tratamento: Toda operação realizada com dados pessoais dentro de seu ciclo de vida, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- Usuário Administrador: pessoa cadastrada no app para, entre outras funções, criar, modificar e excluir Usuários.
- Usuário Simples: toda pessoa autorizada pelo Usuário Administrador a operar os recursos do app em seu nome, por meio de login e senha criados pelo Usuário Administrador.

12.4. TERMOS DE USO

Estes Termos de Uso são aplicáveis a todos os Sites e Aplicativos da ENGECOMP (inclusive sites e aplicativos institucionais e de produtos) e a todos que acessam os nossos Sites e Aplicativos.

Ao acessar os Sites e Aplicativos, você expressamente aceita e concorda com as disposições destes Termos de Uso para todos os Sites e Aplicativos da ENGECOMP. Por conta disso, você deve ler atentamente esses Termos de Uso antes de usar os nossos Sites e Aplicativos. Caso você não concorde com os Termos de Uso, você não deve usar os nossos Sites e Aplicativos.

12.5. ATUALIZAÇÃO DOS TERMOS DE USO

Lembramos que os Termos de Uso, assim como os conteúdos e funcionalidades dos nossos canais poderão ser atualizados a qualquer momento por razões legais, pelo uso de novas tecnologias e funcionalidades e sempre que a ENGECOMP entender que as alterações são necessárias. **Ao continuar a acessar nossos Sites e Aplicativos após as alterações, que serão publicadas nos Sites e Aplicativos, você concorda com as alterações também.**

12.6. TERMOS E CONDIÇÕES DE USO ESPECÍFICOS

Além desses Termos de Uso e Política de Privacidade, alguns Sites e Aplicativos podem ter serviços e funcionalidades específicos e termos e condições adicionais para a sua utilização. Nesse caso, os termos adicionais estarão disponíveis em referidos Sites e Aplicativos e serão aplicáveis se você usar tais serviços e funcionalidades.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

12.7. ACESSO A CONTEÚDO RESTRITO

Alguns dos nossos Sites e Aplicativos possuem área de conteúdo aberto e de conteúdo restrito. Para ter acesso ao conteúdo restrito, pode ser necessário que o Usuário faça um cadastro fornecendo algumas informações pessoais para poder criar um login e senha.

Fique atento se as informações fornecidas estão corretas, pois você é responsável pela veracidade delas, e caso tenha alguma inconsistência, pode impactar no seu acesso ao Site ou Aplicativo.

Como meus dados de cadastro são utilizados?

Você pode conferir os dados pessoais coletados e como são usados em nossa Política de Privacidade.

Posso compartilhar meu login e senha e com terceiros?

Somente você pode utilizar o seu login e senha, sendo assim proibido o compartilhamento com terceiros. Note que o seu acesso é pessoal e intransferível, e você é inteiramente responsável pela guarda, sigilo e bom uso do seu login e senha.

12.8. CONTEÚDOS ENVIADOS POR USUÁRIOS

Alguns de nossos Sites e Aplicativos podem permitir que os Usuários enviem conteúdos como comentários, imagens, mensagens, fotos etc., para divulgação em áreas de conteúdo aberto dos Sites e Aplicativos. Para estes casos, os conteúdos enviados e a identificação do seu perfil, se houver, poderão ser visualizados por outros Usuários, atendendo sempre as normas de sigilo bancário.

Pode também ser possível ao Usuário enviar conteúdo, como fotos, documentos, comentários e outras mensagens para fins de cadastro, atendimento, para uso de serviços disponíveis nos Sites e Aplicativos ou outras finalidades. Nesses casos, os conteúdos enviados não ficarão disponíveis em áreas de conteúdo aberto dos Sites e Aplicativos.

Lembramos que, em qualquer dos casos, os conteúdos enviados serão de responsabilidade de quem os enviou.

12.9. ENVIO DE COMUNICAÇÕES PELO APLICATIVO

Para te manter informado sobre sua conta, produtos e serviços da ENGECOMP, além de informações sobre segurança, poderemos te mandar mensagens pelo aplicativo do celular (push). Caso não queira receber notificações em seu celular, você poderá desabilitar o recebimento nas configurações do seu sistema operacional. Se tivermos uma informação muito importante para lhe passar, enviaremos a mensagem mesmo com a permissão desabilitada.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

12.10. LINKS PARA SITES E APLICATIVOS DE TERCEIROS

Nossos Sites e Aplicativos podem conter links para sites e aplicativos de terceiros. Note que dentro destes sites e aplicativos de terceiros você estará sujeito a outros termos de uso e políticas de privacidade. Nossos Termos de Uso e Política de Privacidade não são válidos nos sites e aplicativos de terceiros. A existência desses links não significa nenhuma relação de endosso ou de patrocínio entre a ENGECOMP e esses terceiros, e a ENGECOMP não tem nenhuma responsabilidade com relação a tais terceiros.

12.11. USOS NÃO PERMITIDOS DOS SISTEMAS E APP DA EMPRESA

A Plataforma deve ser usada de maneira responsável, prudente e cuidadosa, somente para as finalidades para as quais foi concebida, sendo vedado o seu uso para:

a) prática de atos que causem ou possam causar algum tipo de dano ou prejuízo e/ou que violem os direitos das PARTES, seus parceiros, usuários, de quaisquer terceiros ou que violem a ordem pública;
b) finalidades consideradas ilícitas, ilegais, fraudulentas ou prejudiciais, ou com relação a qualquer atividade ou propósito ilícito, ilegal, fraudulento ou prejudicial;
c) prática de atos considerados ameaçadores, maliciosos, abusivos, ofensivos, difamatórios, de assédio, obscenos ou indecentes, ou que promovam o ódio, incitem a violência ou intolerância racial, política ou religiosa;
d) prática de atos que acarretem ou possam acarretar dano ou prejuízo à Empresa, a terceiros, ao app e sistemas da Empresa, à sua disponibilidade ou acessibilidade, ou ainda, que possam danificar, desabilitar, sobrecarregar ou prejudicar os servidores ou redes, ou interferir no seu uso e controle;
e) copiar, modificar, adaptar, traduzir, ou fazer a engenharia reversa de qualquer de sua parte e conteúdo;
f) remover notificações ou citações de qualquer direito autoral, marca registrada ou outros direitos de propriedade contidos na Plataforma ou em qualquer conteúdo ou outro material disponível na Aplicação ou sistema;
g) transmitir arquivos que contenham vírus, “malware”, código incapacitante, arquivos corrompidos ou qualquer outro software ou programa similar que possa danificar a operação do computador de uma outra parte ou para “hackear” ou violar qualquer medida de segurança;
h) disponibilizar ou disseminar informações ou qualquer conteúdo não solicitado ou não autorizado, tais como “SPAM” ou conteúdo pertencente a terceiros e que não tenha direito de utilizar, como, por exemplo, conteúdo protegido por direitos autorais ou conteúdo contendo dados pessoais de terceiros;
i) criar contas de acesso por meios automatizados ou com pretensões falsas ou fraudulentas;
j) utilizar robôs, “spider”, “crawler”, “scraper” ou outros meios ou interfaces automatizadas para acessar a Aplicação ou sistema ou extrair informações de outras pessoas que utilizem a Aplicação ou sistema; ou
k) utilizar a Aplicação ou sistema para a prática de atos que violem padrões éticos e morais ou as normas legais aplicáveis, sendo de todo vedada a distorção da finalidade dos serviços. Exemplificativamente, não serão permitidos a prática de atos que: (i) violem a privacidade e a honra ou que denigram e prejudiquem terceiros; (ii) violem direitos de propriedade intelectual de terceiros; (iii) tenham por objetivo obter o acesso ilegal a dados nossos ou de terceiros; ou (iv) induzam terceiros a erros.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Sem prejuízo das demais hipóteses previstas nestes Termos de Uso, a EMPRESA poderá imediatamente suspender, interromper, bloquear, encerrar ou cessar o seu acesso à Aplicação ou sistema sem necessidade de aviso prévio, em caráter temporário ou permanente, de acordo com a gravidade, nos seguintes casos:

a) Prática ou suspeita de prática de quaisquer um dos atos descritos anteriormente;
b) Violação ou suspeita de violação da legislação vigente ou de quaisquer das demais disposições destes Termos de Uso;
c) Se necessário em razão de restrições técnicas, estratégicas, legais ou comerciais;
d) Se necessário para garantir questões relacionadas à segurança, especialmente no que diz respeito a canais de comunicação, equipamentos ou informações;
e) Caso exigido por suas operações de gerenciamento, manutenção, reparos, modificação ou atualização dos equipamentos, sistemas ou quaisquer das funcionalidades da Aplicação ou sistema; ou
f) Em outras circunstâncias devidamente justificadas.

Além das medidas previstas neste Termos de Uso, a **EMPRESA** poderá também fazer uso de todo e qualquer recurso técnico disponível ou mesmo adotar medidas judiciais cabíveis para impedir a prática dos atos descritos neste capítulo e a violação destes Termos de Uso.

12.12. SOBRE O USO DA APLICAÇÃO OU SISTEMA

Para o emprego da Aplicação ou sistema devem ser observadas as seguintes regras, como segue:

1. **Aceite Formal:** O Consentimento por parte do USUÁRIO ou “aceite as regras de operação da Aplicação ou sistema” representa a manifestação inequívoca de ciência e concordância com todas as disposições aqui descritas, constituindo condição indispensável para o acesso e utilização da plataforma.
2. **Alterações nas Regras**: Em caso de mudança nas normas reguladoras ou orientações de órgãos oficiais, estes termos de uso podem ser ajustados, o que impõe obrigação às PARTES a se manterem atualizadas e em conformidade.
3. **Atualização do cadastro:** O **USUÁRIO** deverá manter sempre seu cadastro devidamente atualizado, especialmente seu endereço e informações de contato.
4. **Autorização para o uso da plataforma:** O **USUÁRIO** declara que está devidamente autorizado pela **EMPRESA** Contratante a preencher seu cadastro, acessar a Plataforma ou serviços dos Parceiros.
5. **Proteção de Dados:** As partes devem garantir que todas as informações inseridas relativas a usuários e prestação de contas sejam tratadas em conformidade com a LGPD (Lei Geral de Proteção de Dados).
6. **Registro e Auditoria:** A Aplicação ou sistema mantém registros auditáveis das promoções, com histórico de alterações e acesso a documentação exigida pela legislação.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

12.13. RESPONSABILIDADES DAS PARTES

Embora a EMPRESA trabalhe para assegurar que a Aplicação ou sistema e seu conteúdo sejam confiáveis, nenhuma garantia (explícita ou implícita) é feita quanto à sua exatidão, integridade ou imparcialidade e, portanto, o USUÁRIO deve, se necessário, obter uma verificação independente de quaisquer das informações nele contidas.

O USUÁRIO e a empresa no qual é vinculado (CONTRATANTE) são os únicos e exclusivos responsáveis pelo uso que fizerem da Aplicação ou sistema e pelas informações fornecidas, respondendo, na forma da lei, por eventuais danos que venham a causar a EMPRESA, aos usuários ou a quaisquer terceiros. Principalmente no que diz respeito às informações fornecidas.

A Aplicação ou sistema poderá sofrer interrupções e indisponibilidades motivadas por questões técnicas ou operacionais. Nestes casos, a ENGECOMP envidará os melhores esforços para viabilizar comunicados prévios sobre eventuais interrupções ou indisponibilidades, bem como para reestabelecer a Aplicação ou sistema tão logo seja possível.

São exemplos de causas de interrupções ou indisponibilidades: casos fortuitos ou de força maior; ações danosas de terceiros que impeçam a prestação dos serviços ou a continuidade da Aplicação ou sistema (hacker, vírus etc.); manutenções técnicas periódicas; falta de energia elétrica; falhas nas redes de transmissão de dados; etc.

A Aplicação ou sistema é fornecida na situação em que se encontram, sem garantias de qualquer natureza, expressas ou implícitas.

Links para outros Websites e/ou Aplicativos. O conteúdo de quaisquer websites de terceiros que o USUÁRIO acessar a partir da Aplicação ou sistema está totalmente fora do controle da EMPRESA, sendo que o acesso e a permanência em tais sites se darão por sua conta e risco. A eventual inclusão destes links na Aplicação ou sistema não implica em endosso ou anuência a quaisquer produtos, serviços, conteúdo, informação ou materiais oferecidos por, ou acessível a nos websites de terceiros. A EMPRESA não representa ou garante quaisquer websites de terceiros que venham a ser acessados a partir da Aplicação ou sistema.

Todos os direitos autorais e marcas comerciais acessíveis através de eventuais links são de propriedade dos respectivos donos dos websites ou dos seus licenciadores.

Os websites de terceiros poderão ter termos de uso e política de privacidade próprios.

12.14. DIREITOS DE PROPRIEDADE INTELECTUAL

Os elementos e/ou ferramentas encontrados na Aplicação ou sistema são ou de titularidade da, ou licenciados à Empresa, sujeitos às normas de propriedade intelectual de acordo com as leis brasileiras e tratados e convenções internacionais dos quais o Brasil seja signatário. Apenas a título exemplificativo, entendem-se como tais: textos, softwares, scripts, imagens gráficas, fotos, sons, músicas, vídeos, recursos interativos e similares, marcas, marcas de serviços, logotipos e “look and feel”.

Caso seja disponibilizada a opção de download de qualquer aplicativo de software ou através de qualquer outro meio, será concedida uma licença não exclusiva, intransferível, não-sublicenciável, para usar o aplicativo em conexão com os

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

serviços relevantes, observadas as disposições destes Termos de Uso, pelo período de duração da Aplicação ou sistema. Não se deve decompilar, desmontar, fazer engenharia reversa ou qualquer outra tentativa de descobrir o código fonte de qualquer parte de referida aplicação, nem permitir que quaisquer terceiros o façam.

As PARTES poderão apresentar sugestões de modificações da Aplicação ou sistema. A EMPRESA poderá incorporar tais modificações e informações adicionais a Aplicação ou sistema a seu exclusivo critério, nada sendo devido as PARTES por tal decisão.

12.15. MEDIDAS DE SEGURANÇA

A ENGECOMP implementa medidas técnicas e organizacionais para proteger os dados pessoais contra perda, roubo, acesso não autorizado e uso indevido. Realiza avaliações de riscos e mantém os sistemas atualizados para garantir a segurança contínua dos dados.

A ENGECOMP tem sua operação tecnológica certificada pela norma ISO 27001 e aplica os padrões mais rigorosos do mercado para governança e salvaguarda dos seus dados conforme apresentados por modelos como COBIT, ITIL, NIST CSF e CIS.

A infraestrutura de segurança utiliza ferramentas e recursos qualificados pelo mercado e constantemente atualizadas para garantir velocidade e qualidade de resposta em caso de ataques ou falhas de segurança.

A empresa também conta com equipes especializadas em engenharia de software, segurança cibernética, privacidade de dados, bem como com contratos de seguro cibernético.

12.16. USO DE COOKIES

Para oferecer a melhor experiência durante a navegação e uso dos serviços da Aplicação ou sistema, pode-se usar cookies para:

a) Garantir maior segurança durante a navegação;
b) Aperfeiçoar a usabilidade, experiência e interatividade na utilização dos serviços;
c) Prover informações mais assertivas e relevantes às necessidades e interesses dos usuários;
d) Buscar maior eficiência em relação à frequência e continuidade da comunicação com os usuários.
e) Responder as dúvidas e solicitações;
f) Realizar pesquisas para melhorar os produtos e serviços, bem como apuração de estatísticas em geral.

A qualquer momento o usuário pode ativar em seu navegador mecanismos para informá-lo, quando eles estiverem acionados ou, ainda, para impedir que sejam utilizados.

Os cookies, arquivos criados pelos websites que, enquanto se navega na Internet, são armazenados no navegador do usuário. A navegação pode se tornar limitada e algumas funcionalidades dos sites podem ficar comprometidas.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

Caso a sua opção de configuração seja recusar cookies, tal ferramenta será desabilitada durante a sua navegação. Caso você aceite o uso dos cookies entenderemos que concordou com as regras conforme descrito neste documento.

12.17. REFERÊNCIAS LEGAIS E NORMATIVAS

A EMPRESA se compromete a seguir regras de privacidade, proteção de dados, confidencialidade ou requisitos de segurança de informações, em conformidade com as seguintes diretrizes legais:

a) LGPD, Lei Geral de Proteção de Dados Pessoais –, lei nº 13.709, de 14 de agosto de 2018;
b) Lei nº 10.406 de 10 de janeiro de 2002 (Código Civil);
c) lei nº 9.609, de 19 de fevereiro de 1998 (Propriedade intelectual de programa de computado);
d) lei nº 9.279, de 14 de maio de 1996 (Propriedade industrial);
e) lei nº 9.610, de 19 de fevereiro de 1998 (Direitos autorais);
f) Lei 12.965/2014, (Marco Civil da Internet)
g) Código Penal, art. 151, 152, 154, 154-A, 298, 307, 207, 184p3, 266.
h) Lei nº 9.296/96, art. 10 (Lei das Interceptações Telefônicas);
i) Lei 7.492/86 art 18 (violação do sigilo de operações)
j) Lei 12.846/2013 (Lei Anticorrupção)
k) Lei 8.069/90 (Estatuto da Criança e do Adolescente)
l) Lei 12.853/2013 (Lei dos direitos autorais)
m) Lei 9.605/98 (Lei de crimes ambientais)
n) Lei 8.078/90 (Código do Consumidor)
o) Decreto-Lei nº70.951/1972
p) Portaria MF nº41/2008
q) ABNT NBR ISO_IEC_20000
r) ABNT NBR ISO_IEC_27000
s) ABNT NBR ISO_IEC_31.000
t) Framework COBIT
u) Framework ITIL

Se eventual determinação legal anular ou tornar ineficaz qualquer das disposições destes Termos e Condições, permanecerão válidas as suas demais condições, salvo caso o efeito da referida determinação.

Em nenhuma circunstância a ENGECOMP ou qualquer de seus parceiros poderão ser responsabilizadas por qualquer delito, negligência, descumprimento contratual ou outra hipótese de ilícito civil ou penal que venham a ser causados por você, sendo de sua total responsabilidade arcar com todos e quaisquer danos, monetários ou de outra natureza, decorrentes de sua atuação indireta, direta ou incidental, cabendo à Empresa o direito de regresso por tais situações.

Como exposto no capítulo “Medidas de Segurança”, a ENGECOMP busca sempre manter medidas de segurança técnicas, físicas e administrativas para fornecer proteção razoável para os dados pessoais contra perda, mau uso, acesso não autorizado, divulgação e alteração. Ainda que se mantenha essas medidas, cada PARTE deve manter em segurança suas informações, bem como se utilizar apenas de ambiente e equipamentos seguros para realizar as conexões necessárias.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

12.18. ALTERAÇÕES NESTE TERMOS DE USO

A ENGECOMP se reserva no direito de modificar, suspender, terminar ou descontinuar qualquer aspecto da Aplicação ou sistema a qualquer tempo, no todo ou em parte. Também poderá impor limitações a certas características, funcionalidades ou serviços sem prévia notificação e sem que isso implique em qualquer responsabilidade por parte da ENGECOMP.

Quaisquer melhorias ou adições à Aplicação ou sistema estarão sujeitos a estes Termos de Uso, a não ser que estabeleçamos de outra forma. A ENGECOMP poderá introduzir novos conjuntos específicos de Termos de Uso para Serviços específicos, conforme apropriado, ou emendar Termos de Uso específicos existentes.

Reserva-se a ENGECOMP o direito de atualizar este documento para refletir mudanças em seus serviços em conformidade com os contratos com seus clientes e a legislação aplicável.

Sempre será fornecida a versão mais recente no site da ENGECOMP.

12.19. PROPRIEDADE INTELECTUAL

Os seguintes itens pertencem a ENGECOMP e somente podem ser usados com sua prévia e expressa autorização:

- todos os softwares, aplicativos ou funcionalidades criadas, produzidos ou contratados pela ENGECOMP para os Sites e Aplicativos, assim como sua identidade visual e conteúdo;
- os nomes das empresas, marcas, patentes, nomes de domínio, slogans, propagandas ou qualquer sinal utilizado para distinguir o que é da ENGECOMP inseridos nos Sites e Aplicativos;

No caso de conteúdos que você enviar ou transmitir pelos Sites e Aplicativos, você autoriza a ENGECOMP a utilizar os direitos intelectuais sobre eles em caráter irrevogável, sem qualquer restrição ou limitação de qualquer natureza.

A utilização, pela ENGECOMP, destes conteúdos enviados por você observará o previsto neste dispositivo. Você também garante que os conteúdos por você enviados não infringem direitos de terceiros.

12.20. SUSPENSÃO DE ACESSO

A qualquer momento, sem aviso prévio ou posterior, a ENGECOMP poderá suspender, cancelar ou interromper o acesso aos Sites e Aplicativos, inclusive se o uso destes canais contrariar o disposto neste documento.

12.21. DISPOSIÇÕES GERAIS

A Empresa poderá ceder a presente relação contratual ou os direitos dela derivados a qualquer das empresas componentes do grupo econômico do qual faz parte, a seu exclusivo critério, bem como a quaisquer terceiros em razão de fusão, cisão, incorporação ou qualquer ato de reestruturação societária.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

A inscrição ou participação na Aplicação ou sistema não gera qualquer vínculo entre os usuários e a Empresa, que não aquele expressamente previsto nestes Termos de Uso.

Fica desde já eleito o foro da comarca de São Paulo/SP para dirimir quaisquer conflitos relacionados a estes Termos de Uso, por mais privilegiado que outro possa ser ou vir a ser.

Data da última atualização: 11/08/2025

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

13. POLÍTICA PARA MANUSEIO DE DADOS PESSOAIS

13.1. OBJETIVO

A presente Política para Manuseio de Dados Pessoais ("Política") tem como objetivo determinar as regras internas para o Manuseio de Dados Pessoais na ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente "Empresa".

Para os fins da presente Política, deve-se entender por Manuseio de Dados Pessoais:

Toda a operação de tratamento de Dados Pessoais, como, por exemplo, a coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, atualização, comunicação, transferência, compartilhamento e extração.

13.2. RESPONSABILIDADES

Compete ao Encarregado:

- Analisar e aprovar ou reprovar as solicitações de suspensão de prazo de armazenamento de Dados Pessoais;
- Analisar situações em que os Dados Pessoais de crianças poderão ser manuseados sem o Consentimento de um dos pais ou responsável legal;
- Elaborar Relatório de Impacto à Proteção de Dados Pessoais, quando necessário.
- Manter o registro das operações de Manuseio de Dados Pessoais, contemplando a respectiva Base Legal.

Compete à Área responsável pelo Manuseio de Dados Pessoais

- Observar e atender as regras definidas nesta Política, quando aplicáveis.

13.3. REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

Todas as operações de Tratamento de Dados Pessoais devem ser registradas em documento específico para tal fim, que contenha, no mínimo:

a) A área responsável pelo tratamento;
b) A finalidade do tratamento;
c) Quais Dados Pessoais são tratados;
d) De quem são os Dados Pessoais tratados (cliente, corretor, fornecedor, Colaboradores etc.);
e) Se há o tratamento de Dados Pessoais de crianças;
f) Se há o compartilhamento desses dados com Terceiros (inclusive transferência internacional);
g) Base legal autorizadora do tratamento.

É obrigação do Encarregado pela Proteção de Dados Pessoais manter o registro das atividades de tratamento de Dados Pessoais atualizado.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Sempre que julgar necessário, o Encarregado poderá solicitar informações adicionais à área responsável pelo tratamento dos Dados Pessoais, especialmente, para a realização de monitoramento e fiscalização.

13.4. REGRAS GERAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Em toda e qualquer operação de tratamento de Dados Pessoais, sejam eles obtidos diretamente do Titular, de Terceiros ou de bases públicas, deverão ser observadas as seguintes regras:

- **Finalidade**: O Manuseio de Dados Pessoais deverá ser realizado unicamente para o cumprimento de uma finalidade específica, pré-determinada e informada ao Titular;
- **Necessidade:** O Manuseio deverá ser restrito ao mínimo de Dados Pessoais necessário para o alcance da finalidade pré-definida;
- **Não Discriminação:** O Manuseio de Dados Pessoais não poderá ser realizado para fins discriminatórios ilícitos;
- **Qualidade**: A ENGECOMP deverá se atentar para a precisão, qualidade e acurácia dos dados que manuseia.
- **Transparência:** Deverá ser garantida a transparência ao Titular sobre o Tratamento de seus Dados Pessoais.

13.5. COMPARTILHAMENTO DE DADOS PESSOAIS

Ao compartilhar Dados Pessoais com Terceiros, (enviar ou receber dados), deverão ser observadas as regras estabelecidas na Política de Compartilhamento de Dados Pessoais.

13.6. ARMAZENAMENTO DE DADOS PESSOAIS

Os documentos que contenham Dados Pessoais não poderão ser armazenados por período superior ao necessário para o cumprimento da finalidade pretendida, independentemente do formato utilizado, se físico ou eletrônico.

13.7. DADOS PESSOAIS SENSÍVEIS

No Manuseio de Dados Pessoais sensíveis, deverão ser observadas as hipóteses autorizadoras específicas para tanto. São Dados Pessoais sensíveis aqueles relativos à:

- Origem racial ou étnica;
- Convicção religiosa;
- Opinião política;
- Filiação a sindicato;
- Organização de carácter religioso, filosófico ou político;
- Saúde ou à vida sexual; e
- Dado genético ou biométrico.

No caso de dúvidas sobre a classificação de qualquer Dado Pessoal como sensível, o Encarregado deverá ser consultado.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

13.8. DADOS PESSOAIS DE CRIANÇAS

O Manuseio de Dados Pessoais de crianças, deverá ser realizado:

- Em seu melhor interesse, ou seja, com a finalidade de beneficiá-las, ainda que de forma indireta;
- Com transparência, considerando as condições físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos destinatários, com o uso de recursos audiovisuais, quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança, conforme Norma de Transparência ao Titular.

O tratamento de Dados Pessoais de crianças necessitará da prévia coleta do consentimento específico e em destaque, de pelo menos um dos pais ou responsáveis legais.

Na hipótese de necessidade de contatar os pais ou representante legal da criança, os Dados Pessoais poderão ser coletados sem o consentimento prévio, desde que não sejam armazenados, e utilizados apenas uma única vez.

Outras exceções deverão ser aprovadas pelo Encarregado.

13.9. HIPÓTESES AUTORIZADORAS PARA O TRATAMENTO DE DADOS PESSOAIS

Para que uma atividade de tratamento de Dados Pessoais possa ser realizada, ela deve ser fundamentada em uma das hipóteses autorizadoras (bases legais) abaixo:

Cumprimento de Obrigação Legal ou Regulatória

Existência de lei, norma, decisão judicial ou regulação vigente, pela qual o tratamento se torna obrigatório (e não opcional). Exemplos:

- Arquivamento de notas fiscais;
- Manutenção de documentos conforme exigências do Banco Central, SUSEP, CVM e B3;
- Controle de ponto de Colaboradores;
- Envio de dados ao E-Social.

Execução de Contrato ou Procedimentos preliminares ao contrato

Quando necessário o tratamento para a execução de contrato ou de procedimentos preliminares relacionados a um contrato, do qual o Titular seja parte. Exemplos:

- Entrega de produtos e prestação de serviços aos clientes;
- Atendimento a clientes;
- Recrutamento e seleção;
- Pagamento de Colaboradores;
- Fornecimento de benefícios aos Colaboradores.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

Exercício Regular de Direito

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, em trâmite ou futuro. Exemplos:

- Arquivo de processos judiciais;
- Arquivo de documentos para defesa em processos trabalhistas;
- Procurações para atuação em processos judiciais ou administrativos;
- Documentos de comprovação para obtenção de benefícios fiscais.

Para o tratamento de dados sensíveis, a legislação prevê que o exercício regular de direito também será aplicável no âmbito contratual.

Tutela da Saúde

Para garantir a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, sendo vedado qualquer outro uso que desvirtue essa finalidade. Exemplos:

- Procedimentos de Medicina do Trabalho;
- Exames laboratoriais.

Proteção da Vida ou Incolumidade Física

Para garantir a proteção da vida ou incolumidade física do Titular ou de Terceiros, quando em iminente perigo. Exemplo, em atendimentos médicos de emergência.

Proteção ao Crédito

Para garantir a proteção ao crédito, observando-se a legislação vigente (como: Lei do Cadastro Positivo e Código de Defesa do Consumidor). Exemplos:

- Consultas a cadastros para concessão de crédito;
- Manutenção de histórico de adimplementos para futuras concessões de crédito.

Prevenção à Fraude e à Segurança do Titular

Para prevenção à fraude e à segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Exemplos:

- Fechaduras/catracas biométricas;
- Reconhecimento facial em cadastros de acesso, com a finalidade de garantir a segurança.

Essa base legal se encontra prevista exclusivamente para as hipóteses de tratamento de Dados Pessoais sensíveis.

Legítimo Interesse

Para garantir a continuidade da atividade econômica/operação dos agentes de tratamento, desde que o Titular dos dados tenha expectativa quanto à atividade de tratamento. Exemplos:

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Estudos e relatórios internos sobre as atividades da empresa;
- Avaliações de desempenho de Colaboradores;
- Oferta de serviços adicionais a Titulares que já são clientes (Usuários);
- Auditorias internas.

É importante destacar que o tratamento de Dados Pessoais com base em interesses legítimos não será permitido, caso ameace ou lesione direitos e liberdades fundamentais do Titular.

Quando o tratamento for realizado com base no legítimo interesse, o Encarregado poderá elaborar Relatório de Impacto à Proteção de Dados Pessoais, quando necessário.

Consentimento

Pode ser utilizado para fundamentar qualquer atividade de tratamento, desde que seja livre, informado e inequívoco. Contudo, o tratamento realizado com base unicamente no consentimento fica restrito à vontade do Titular, que pode, a qualquer tempo, revogá-lo.

Nos casos em que a base legal adequada para o tratamento seja o consentimento, deverá ser observado o Procedimento Corporativo para Gestão e Uso do Consentimento.

13.10. PENALIDADES

O cumprimento de todas as Políticas publicadas é exigido de todos os Colaboradores da ENGECOMP, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

13.11. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato com o Encarregado pelo Tratamento de Dados Pessoais da empresa pelo e-mail dpo@engecomp.com.br.

O cumprimento deste Procedimento é de suma importância e dever de todos. Em caso de não observância deste procedimento, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: dpo@engecomp.com.br.

As denúncias de violações às Políticas e Procedimentos serão anônimas e a não-retaliação será garantida.

13.12. EXCEÇÕES

Não se aplica.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

13.13. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política para Uso e Gestão do Consentimento;
- Regimento Interno do Comitê de Privacidade e Proteção de Dados Pessoais;
- Código de Conduta;
- Política De Organização De Trabalhos Orientados A Privacidade De Dados

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

14. POLÍTICA DE COMPARTILHAMENTO DE DADOS PESSOAIS COM TERCEIROS

14.1. OBJETIVO

O objetivo do presente Procedimento Corporativo de Compartilhamento de Dados Pessoais é determinar as regras aplicáveis ao Compartilhamento de Dados Pessoais que sejam de conhecimento da ENGECOMP com Terceiros.

Para os fins do presente Procedimento, considera-se Compartilhamento de Dados com Terceiros toda a comunicação, difusão, transferência (inclusive internacional), interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Exemplos:

- Armazenamento destes dados em serviços de cloud;
- Transferência de Dados Pessoais para empresas parceiras, a fim de executar serviços contratados por um Titular;
- Envio de relação de Colaboradores para fornecedores de benefícios.

O Compartilhamento de Dados Pessoais com Terceiros somente poderá ser realizado para o atendimento da finalidade previamente informada ao Titular, através do Aviso de Privacidade ou outro meio que garanta a transparência do tratamento.

É responsabilidade do Gestor da Área que realiza o Compartilhamento garantir que estas determinações sejam devidamente cumpridas.

14.2. RESPONSABILIDADES

Compete ao Encarregado:

- Aprovar o Relatório descrito no item “RELATÓRIO DE AVALIAÇÃO” desta política, emitido pelo Gestor da Área Solicitante/Responsável pelo Compartilhamento, nos casos de operações com níveis de exposição baixo e médio;
- Emitir o parecer a respeito do Relatório descrito no item “RELATÓRIO DE AVALIAÇÃO desta Política, e submetê-lo à aprovação da subcomissão de Segurança e Privacidade, nos casos de operações com níveis de exposição alto e muito alto;
- Realizar o acompanhamento periódico/monitoramento das operações de Compartilhamento, tomando as medidas necessárias para mitigar eventuais riscos identificados;
- Nas operações de Compartilhamento de sensibilidade crítica, assegurar-se que:

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

  - o grau de proteção de Dados Pessoais do país destinatário tenha sido reconhecido pela ANPD como adequado ao previsto na legislação brasileira vigente; e
  - o Terceiro destinatário garanta o cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados adotado pela legislação brasileira vigente;
- Manter o registro das operações de Compartilhamento com Terceiros, contemplando a respectiva Base Legal e elaborar o Relatório de Impacto à Proteção de Dados Pessoais, quando entender necessário;
- Garantir que as diligências prévias e necessárias ao Compartilhamento de Dados Pessoais tenham sido observadas pela Área responsável pelo Compartilhamento;
- Armazenar o registro relativo às diligências para o Compartilhamento de Dados Pessoais, realizadas pela Área responsável pelo Compartilhamento.

Compete à Área responsável pelo Compartilhamento:

- Observar e atender as diretrizes definidas nesta política, quando aplicáveis.
- Realizar e documentar as diligências prévias e necessárias ao Compartilhamento de Dados Pessoais com Terceiros, com o intuito de comprovar a adequação dos seus procedimentos frente a auditorias, testes de controle, fiscalizações, entre outras situações;
- Emitir o Relatório de avaliação descrito nesta política, e submetê-lo ao Encarregado para aprovação ou emissão de parecer.

Compete a Assessoria Jurídica e a Subcomissão de Segurança e Privacidade:

- Observar os requerimentos regulatórios locais e os padrões de cláusulas contratuais da Companhia, quando da redação ou revisão das cláusulas dos contratos firmados com Terceiros.
- Assegurar, quando pertinente, que os contratos contemplem cláusulas que resguardem os direitos dos titulares e os interesses da Companhia, relativos à privacidade e proteção de dados pessoais.

14.3. CENÁRIOS DE COMPARTILHAMENTO

O Compartilhamento de Dados Pessoais com Terceiros deverá ser classificado de acordo com o grau de exposição do dado pessoal. Esta classificação deverá ser realizada pelo próprio Gestor da Área Solicitante/Responsável pelo Compartilhamento, com o auxílio do Encarregado, quando necessário. A escala a seguir se propõe a orientar essa classificação.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Grau de Exposição	Quem pode autorizar o compartilhamento	Descrição do grau de exposição do dado pessoal
Muito baixo	Gestor da área ou responsável pelo compartilhamento	Quando há compartilhamento de Dados Pessoais Anonimizados ou estatísticos que não possibilitam a identificação de um Titular de Dados.
Baixo	Encarregado	Quando um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
Médio	Subcomissão de privacidade e Diretoria Executiva	Quando há o compartilhamento de Dados Pessoais sem qualquer procedimento para mascaramento ou vínculo direto com o titular.
Alto	Subcomissão de privacidade e Diretoria Executiva	Quando há compartilhamento de Dados Pessoais classificados como: (i) Dados Pessoais Sensíveis; (ii) Dados Pessoais de criança e adolescente; (iii) Dados Pessoais Financeiros; (iv) Dados Pessoais de Comportamento.
Muito alto	Subcomissão de privacidade e Diretoria Executiva	Quando há Compartilhamento/Transferência Internacional de Dados Pessoais.

14.4. REGRAS GERAIS PARA TODAS AS ATIVIDADES DE COMPARTILHAMENTO DE DADOS PESSOAIS

Em regra, toda a atividade que envolva o Compartilhamento de Dados Pessoais deverá ser embasada em contrato ou aditivo contratual.

A subcomissão de Segurança e Privacidade, em linha com a área jurídica da ENGECOMP deverá assegurar, quando pertinente, que os contratos contemplem cláusulas que resguardem os direitos dos titulares e os interesses da ENGECOMP, relativos à privacidade e proteção de dados pessoais.

Sempre que julgar necessário, o Encarregado poderá solicitar a realização de auditoria para garantir que o Terceiro está observando todas as regras previstas em Contrato.

Caso, não seja possível a formalização de um contrato ou aditivo contratual, o compartilhamento de dados deverá, obrigatoriamente, ser aprovado pelo Subcomissão de Segurança e Privacidade e por uma Diretoria Executiva da ENGECOMP (por exemplo, envio de Dados Pessoais para o INSS).

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

14.5. REGRAS ESPECÍFICAS PARA O COMPARTILHAMENTO DE DADOS PESSOAIS, CONSIDERANDO O NÍVEL DE SENSIBILIDADE DA OPERAÇÃO

Deverão ser observadas as disposições estabelecidas no item acima e, adicionalmente, para cada nível de sensibilidade, as seguintes regras:

- **Compartilhamento de grau de exposição Muito Baixa:** Quando a empresa compartilhar dados Anonimizados, deverá estar garantido em contrato que o Terceiro se comprometerá a manter a Anonimização dos dados compartilhados, sendo vedado o cruzamento de qualquer base de dados que resulte em possível identificação dos Titulares.
- **Compartilhamento de grau de exposição Baixa:** O Gestor da Área Solicitante/Responsável pelo compartilhamento deverá elaborar o Relatório previsto no item a seguir.1 deste Procedimento e submetê-lo para a aprovação do Encarregado.
- **Compartilhamento de grau de exposição Médio:** O Gestor da Área Solicitante/Responsável pelo compartilhamento deverá elaborar o Relatório previsto no item a seguir deste Procedimento e submetê-lo para a aprovação do Encarregado e para a Subcomissão de Privacidade e Segurança. Se aprovado, o Encarregado deverá realizar, periodicamente, o acompanhamento do compartilhamento dos Dados Pessoais, para garantir que todas as obrigações contratuais relativas à privacidade e proteção de dados estão sendo observadas pelos Terceiros, de acordo com as diligências necessárias apontadas no item DILIGÊNCIAS (abaixo).
- **Compartilhamento de grau de exposição Alta:** O Gestor da Área Solicitante/Responsável pelo compartilhamento deverá elaborar o Relatório de Compartilhamento previsto no item abaixo deste Procedimento e submetê-lo para parecer do Encarregado e da Subcomissão de Privacidade e Segurança. Se aprovado, o Encarregado deverá realizar, periodicamente, o acompanhamento do compartilhamento dos Dados Pessoais, para garantir que todas as obrigações contratuais relativas à privacidade e proteção de dados estão sendo observadas pelos Terceiros, de acordo com as diligências necessárias apontadas no item DILIGÊNCIAS (abaixo).
- **Compartilhamento de grau de exposição Muito Alto:** Toda a transferência de Dados Pessoais para país estrangeiro ou organismo internacional do qual o país seja membro será classificada como Compartilhamento de grau de exposição Muito Alto Crítica. O Gestor da Área Solicitante/Responsável pelo compartilhamento deverá elaborar o Relatório previsto no item a seguir desta Procedimento e submetê-lo para parecer do Encarregado e para a Subcomissão de Privacidade e Segurança. Se aprovado, o Encarregado será responsável por certificar que:
  - O grau de proteção de Dados Pessoais do país destinatário tenha sido reconhecido pela Autoridade Nacional de Proteção de Dados (“ANPD”), como adequado ao previsto na legislação brasileira vigente;
  - O Terceiro destinatário garanta o cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados adotado pela legislação brasileira vigente, na forma de:
    - Cláusulas-padrão contratuais, definidas pela ANPD;
    - Cláusulas contratuais específicas para determinada transferência;
    - Normas corporativas globais;
    - Selos, certificados e códigos de conduta regularmente emitidos.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Na hipótese da aplicação de cláusulas contratuais específicas ou normas corporativas globais, o Encarregado deverá providenciar a sua verificação e aprovação pela ANPD.

14.6. RELATÓRIO DE AVALIAÇÃO

O Gestor da Área Solicitante/Responsável pelo Compartilhamento, quando as operações forem classificadas como de grau de exposição Baixa, Média, Alta e Muito Alta, deverá informar ao Encarregado pela Proteção de Dados Pessoais, por e-mail, as seguintes informações:

a) O propósito/objetivo do Compartilhamento;
b) Os dados que a ENGECOMP precisa compartilhar para atingir a finalidade pretendida;
c) Indicar se é possível atingir a finalidade indicada, sem o Compartilhamento dos Dados Pessoais, ou mediante sua respectiva Anonimização;
d) Indicar o que aconteceria se o dado pessoal não fosse compartilhado;
e) A existência de alguma proibição legal para o compartilhamento dos Dados Pessoais pela ENGECOMP;
f) Quais os riscos identificados em realizar o compartilhamento, considerando as diligências descritas no item "DILIGÊNCIAS" desta política; e
g) Quando e como os Dados Pessoais devem ser compartilhados.

14.7. LIMITAÇÕES AO COMPARTILHAMENTO

Em toda a atividade de compartilhamento de Dados Pessoais, deverão ser observadas as seguintes limitações:

- Compartilhamento de Dados Pessoais Sensíveis de Saúde: Dados Pessoais que se referem à saúde do indivíduo não podem ser compartilhados com Terceiros com finalidade de se obter vantagem econômica; e
- Compartilhamento de Dados Pessoais de Crianças: Dados Pessoais de crianças (até 12 anos) somente poderá ser compartilhado com Terceiros mediante consentimento dos pais ou responsável(eis).

14.8. DILIGÊNCIAS

O Departamento responsável pelo Compartilhamento deverá, previamente ao Compartilhamento, avaliar se o Terceiro:

- Observa as normas relativas à privacidade e proteção de Dados Pessoais;
- Possui um programa de privacidade e proteção de Dados Pessoais;
- Adota as medidas necessárias para garantir a segurança dos Dados Pessoais que manuseia;
- Possui um plano de resposta a incidentes relativo a dados pessoais;
- Já sofreu algum tipo de incidente e/ou autuação relativos ao tratamento de dados pessoais.

O Encarregado deverá monitorar o cumprimento das obrigações relativas à privacidade e proteção de dados pessoais, pelos Terceiros, durante a vigência do contrato e/ou da operação de Compartilhamento.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

14.9. PENALIDADES

O cumprimento de todas as Políticas e Procedimentos publicados é exigido de todos os Colaboradores da ENGECOMP, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

14.10. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo e-mail: dpo@engecomp.com.br.

Em caso de não observância desta política, favor reportar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais, pelo e-mail: dpo@engecomp.com.br

As denúncias de violações às Políticas e Procedimentos serão anônimas e a não-retaliação será garantida.

14.11. EXCEÇÕES

Não se aplica.

14.12. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política de Manuseio de Dados Pessoais;
- Política para Uso e Gestão do Consentimento;
- Código de Conduta;
- Política De Organização De Trabalhos Orientados A Privacidade De Dados

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

15. POLÍTICA DE USO E GESTÃO DO CONSENTIMENTO

15.1. OBJETIVO

A presente Política para Uso e Gestão de Consentimento no Tratamento de Dados Pessoais tem por objetivo determinar as regras aplicáveis ao uso do Consentimento como base legal para o tratamento de Dados Pessoais, devendo ser observada por todos os Colaboradores da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

15.2. ORIENTAÇÕES GERAIS

O Consentimento é uma manifestação do Titular do Dado Pessoal que autoriza o tratamento de seus Dados Pessoais. Para o Consentimento ser válido, deve-se:

- Obedecer a uma finalidade (objetivo) específica, não genérica. Esta finalidade deve ser apresentada ao Titular do Dado Pessoal de maneira clara e antes da coleta do Consentimento. (Por exemplo, “Ao clicar no quadrado abaixo, você autoriza o uso de seu nome e e-mail para envio de e-mails personalizados com anúncios de parceiros”);
- Garantir que se deu de forma livre e inequívoca;
- Destacá-lo das demais disposições e contratuais; e
- Preferencialmente, apresentá-lo de forma granular.

Segue mais considerações sobre termos aplicados ao Consentimento:

- **Consentimento livre:** O Consentimento livre pressupõe que o Titular não tenha sido compelido a autorizar o tratamento dos seus dados. Assim, essa base legal somente será apropriada se, ao Titular, for oferecida uma escolha genuína em relação a aceitar ou recusar os termos oferecidos para o tratamento dos seus dados.
- **Consentimento informado:** Fácil e de imediato acesso às informações sobre como os Dados do Titular serão tratados, os efeitos do fornecimento e discordância da autorização solicitada. A linguagem utilizada deve ser clara e em linguagem de fácil entendimento para o público alvo. Recomenda-se a adoção de mensagens curtas e diretas. O Titular deve ser, no mínimo, informado sobre: (i) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o Consentimento; (ii) quais dados serão coletados e utilizados;
- **Consentimento inequívoco:** para que o Consentimento seja inequívoco, é preciso que este seja dado por meio de uma ação positiva do Titular, ou seja, tem de ser óbvio que o Titular dos dados deu o Consentimento para o tratamento de seus Dados Pessoais. Exemplo: utilização de caixas pré-selecionadas ou utilização de cookies dos usuários que não deram aceites nos avisos externos. Para o Consentimento ser inequívoco é necessário que o Titular tenha uma ação afirmativa para concedê-lo, como marcar o checkbox ou clicar no item de aceite de cookies etc. O responsável pelo tratamento deve se atentar para o fato de que o Consentimento não poder ser obtido através da mesma ação de concordar com o contrato ou aceitar as condições gerais do serviço (comumente chamadas de “Li e Concordo”). A aceitação de condições gerais não pode ser confundida com o ato inequívoco de consentir com o tratamento dos Dados Pessoais.
- Finalidade específica e determinada: Os dados não poderão ser tratados para uma finalidade distinta daquela consentida pelo Titular. Nesse contexto, para que a ENGECOMP obtenha o Consentimento válido, deverá

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

garantir ao Titular máxima transparência sobre a finalidade para a qual pretende tratar os seus Dados Pessoais. Caso a ENGECOMP tenha a intenção de tratar os dados para outra finalidade deverá obter novo Consentimento para a nova finalidade ou certificar-se da existência uma outra base legal que permita este tratamento.

15.3. RESPONSABILIDADES

Compete ao Encarregado:

- Garantir a constante atualização do registro de atividades de tratamento e respectivas bases legais.
- Monitorar periodicamente a atividade de tratamento baseada em Consentimento, para garantir que não houve mudança na finalidade para a qual o Titular deu seu Consentimento;
- Garantir que Dados Pessoais dos Titulares que revogaram seu Consentimento não sejam tratados sem que haja outra base legal que autorize o tratamento;
- Garantir que a empresa disponibiliza método simplificado para que o Titular possa, a qualquer momento, revogar o Consentimento;
- Aprovar as cláusulas/scripts de informação e requisição do Consentimento;
- É de responsabilidade do Encarregado garantir que os registros relativos à obtenção e revogação do Consentimento sejam armazenados e documentados de forma organizada; e
- Monitorar se as solicitações de revogação estão sendo devidamente respondidas e observadas pelos Terceiros.

Compete à área que realiza a atividade de tratamento cuja base legal seja o Consentimento

- Observar e atender as diretrizes definidas nesta Política, quando aplicáveis;
- Adaptar a linguagem e design/layout das informações e da requisição de Consentimento, conforme o seu destinatário e os meios empregados para o registro dos dados e da obtenção do Consentimento (meio telefônico, formulários web, contratos, formulários em suporte físico, entre outros);
- Utilizar as cláusulas/scripts de informação e requisição do Consentimento, previamente aprovados pelo Encarregado;
- Exigir comprovação do vínculo legal entre a criança e aquele que se declara responsável legal e manter as evidências desta verificação, quando obtiver o Consentimento para o tratamento de Dados Pessoais de crianças; e
- Informar ao Titular, o meio para a revogação do Consentimento, bem como garantir meios seguros e facilitados para que o Titular possa revogar esta autorização, sem a necessidade de se apresentar qualquer justificativa.

Compete ao Departamento Jurídico:

- Assegurar, quando pertinente, que os contratos contemplem cláusulas destacadas ou apartadas para a obtenção do Consentimento.

15.4. FORNECIMENTO DE INFORMAÇÕES E OBTENÇÃO DO CONSENTIMENTO

A área responsável pela coleta do Consentimento deverá adaptar a linguagem e design/layout das informações e da requisição de Consentimento, conforme o seu destinatário e os meios empregados para o registro dos dados e da obtenção do Consentimento (meio telefônico, formulários web, contratos, formulários em suporte físico, entre outros).

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Em qualquer caso, as áreas da ENGECOMP que tratem Dados Pessoais com base no Consentimento, deverão usar as cláusulas/scripts de informação e requisição do Consentimento, previamente aprovados pelo Encarregado pela Proteção de Dados Pessoais designado pela empresa. Se o Consentimento for solicitado como parte de contrato, o responsável pela área jurídica da empresa deve assegurar que este seja requerido de maneira destacada ou em documento apartado.

15.5. CONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Dados pessoais sensíveis são informações que versam sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico de um indivíduo.

Quando utilizado para tratar dados sensíveis, além de observar as demais regras previstas nesta Política, o Consentimento deve:

- Se dar de forma específica, ou seja, direcionada exclusivamente para o tratamento de tais informações;
- Ser inserido de maneira destacada dos demais termos e requisições de autorização/contrato.

15.6. CONSENTIMENTO PARA O TRATAMENTO DE DADOS DE CRIANÇAS

Em decorrência da vulnerabilidade de indivíduos menores de 12 (doze) anos de idade, o tratamento de seus Dados Pessoais deverá ocorrer apenas em hipóteses excepcionais e mediante a coleta do Consentimento específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal do indivíduo, este Consentimento poderá ser em folha apartada ou em campo especial e em destaque no documento principal.

Ao coletar o Consentimento de um dos pais ou responsável pela criança, a área que efetivar o tratamento destes dados deverá exigir comprovação do vínculo legal existente entre a criança e aquele que se declara responsável legal e manter as evidências desta verificação.

15.7. O ÔNUS DA PROVA QUANTO AOS REQUISITOS DO CONSENTIMENTO VÁLIDO

É da ENGECOMP a responsabilidade de demonstrar que todos os requisitos necessários para a validade do Consentimento foram devidamente observados, no momento da obtenção do Consentimento junto ao Titular dos dados.

Dessa forma, é necessário que o responsável da área que manuseia Dados Pessoais com base no Consentimento adeque as informações e a requisição do Consentimento ao canal pelo qual o procedimento tenha sido realizado (telefone, online ou presencial), e mantenha integral registro da operação.

Para esses fins, recomenda-se a gravação de chamadas telefônicas, manutenção de cópias dos documentos assinados pelos Titulares dos dados, bem como registros eletrônicos gerados pelas plataformas através das quais os procedimentos tenham ocorrido.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

É de responsabilidade do Encarregado garantir que essas informações sejam armazenadas e documentadas de forma organizada.

15.8. OPOSIÇÃO E REVOGAÇÃO DO CONSENTIMENTO

Deverá ser garantido, ao Titular dos Dados Pessoais, a revogação facilitada do seu Consentimento, quando este assim desejar. Assim, sempre que da coleta do Consentimento, a área responsável pelo tratamento dos Dados Pessoais deverá informar o meio para revogação, bem como garantir meios seguros e facilitados para que o Titular possa revogar esta autorização, sem a necessidade de se apresentar qualquer justificativa.

Caso os Dados Pessoais tenham sido compartilhados com Terceiros, a Área responsável pelo compartilhamento reportará a revogação do Consentimento pelo Titular ao departamento jurídico, que deverá notificar esses Terceiros comunicando o ocorrido e requisitando a interrupção do tratamento dos Dados Pessoais, caso não haja outra base legal que autorize este tratamento.

O Encarregado pela Proteção de Dados Pessoais será responsável por monitorar se as solicitações de revogação estão sendo devidamente respondidas e observadas pelos Terceiros.

15.9. GESTÃO DO CONSENTIMENTO

Para gerir o Consentimento de forma eficiente, o Encarregado pela Proteção de Dados Pessoais deve garantir a constante atualização do registro de atividades de tratamento e respectivas bases legais. Dessa forma, quando um Titular de Dados Pessoais revogar o Consentimento, a ENGECOMP será capaz de identificar a atividade à qual o Titular se refere e responder à sua solicitação de forma assertiva e em prazo razoável.

O Encarregado deverá também:

- Revisar periodicamente a atividade de tratamento baseada em Consentimento, para garantir que não houve mudança na finalidade para a qual o Titular deu seu Consentimento;
- Garantir que Dados Pessoais dos Titulares que revogaram seu Consentimento não sejam tratados sem que haja outra base legal que autorize o tratamento; e
- Garantir que a empresa disponibiliza método simplificado para que o Titular possa, a qualquer momento, revogar o Consentimento.

15.10. PENALIDADES

O cumprimento de todas as Políticas publicadas é exigido de todos os Colaboradores da ENGECOMP, constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares, tais como advertência verbal, escrita ou até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

15.11. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo canal dpo@engecomp.com.br

O cumprimento desta Política é de suma importância e dever de todos. Em caso de não observância desta Política, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: dpo@engecomp.com.br

As denúncias de violações às Políticas e Procedimento serão anônimas e a não-retaliação será garantida.

15.12. EXCEÇÕES

Não se aplica.

15.13. DOCUMENTOS RELACIONADOS

Normativos internos relacionados ao tema, não se limitando a:

- Política de Manuseio de Dados Pessoais;
- Política para Uso e Gestão do Consentimento;
- Código de Conduta;
- Política De Organização De Trabalhos Orientados A Privacidade De Dados

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

16. POLÍTICA DE ORGANIZAÇÃO DE TRABALHOS ORIENTADOS A PRIVACIDADE DE DADOS

16.1. OBJETIVO

A presente política visa orientar a organização de trabalhos e construção de artefatos de processos com suporte das diretrizes de privacidade de dados na ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

16.2. RESPONSABILIDADES

É responsabilidade do Encarregado:

- Emitir parecer sobre a viabilidade do projeto, do ponto de vista de privacidade e proteção de Dados Pessoais;
- Preencher o LIA, quando cabível, para verificar a adequação do Tratamento à Base Legal do Legítimo Interesse;
- Emitir o parecer de recomendação sobre a aprovação ou não do Projeto, de forma clara e compreensível;
- Executar as ações necessárias para a emissão do parecer;
- Dar suporte, quando solicitado, ao gestor responsável pelo Projeto;
- Elaborar um Relatório de Impacto à Proteção de Dados Pessoais (“RIPD"), sempre que entender pertinente, independentemente da sensibilidade do Projeto;
- Manter os registros do processo de aprovação dos Projetos, incluindo o LIA e o Questionário de Avaliação de Grau de Exposição;
- Aprovar ou não os Projetos, quando o gestor do Projeto também for o Gestor da Área responsável pelo Projeto.

Compete aos responsáveis pela aprovação do Projeto:

- Observar as demais normas e regras internas da ENGECOMP, relacionadas ou não à privacidade e proteção de Dados Pessoais;
- Documentar o processo de aprovação e os fundamentos da decisão final;
- Não aprovar o Projeto sem possuir todas as informações necessárias relativas aos graus de exposição apresentados;
- Ater-se às recomendações e conclusões do parecer emitido pelo Encarregado.

Compete ao Gestor do Projeto:

- Observar as demais normas e regras internas da ENGECOMP, relacionadas ou não à privacidade e proteção de Dados Pessoais;
- Responder o Questionário de Avaliação de Grau de Exposição e submetê-lo para parecer do Encarregado.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

16.3. DIRECIONADORES PARA CONSTRUÇÃO DE PROCESSOS E ARTEFATOS

Todos os colaboradores da ENGECOMP deverão observar o seguinte conjunto de direcionares fundamentais para o tratamento de dados pessoais:

- **Finalidade:** O Tratamento de Dados Pessoais deve servir a propósitos legítimos, específicos, explícitos e informados ao Titular, sem possibilidade de Tratamento posterior de forma incompatível com essas finalidades.
- **Limitação de Dados Pessoais e Processamento dos Dados:** Os Dados Pessoais a serem utilizados no Projeto deverão ser relevantes, proporcionais, adequados e necessários para alcançar a finalidade do Projeto.
- **Controle de Acesso:** Os Dados Pessoais empregados no âmbito do Projeto deverão ser administrados de forma a garantir que somente os Colaboradores que necessitem ter acesso aos Dados Pessoais, o tenham.
- **Precisão e Qualidade dos dados:** O Projeto deverá ser concebido de modo que os Dados Pessoais sejam precisos e atualizados para o atingimento da finalidade pretendida com a atividade de Tratamento.
- **Eliminação e Anonimização dos dados ao Final do Processo**: O Projeto deverá prever procedimentos e meios para garantir a eliminação, ou a implementação de solução que permita a Anonimização dos Dados Pessoais.
- **Retenção:** Os Dados Pessoais não deverão ser retidos por mais tempo do que o necessário para o atendimento da finalidade para a qual é tratado.
- **Segurança:** O Projeto deverá passar por análise da área de Segurança da Informação, para garantir que os dados estarão seguros durante todo o seu ciclo de vida.
- **Não Discriminação:** O Projeto não poderá contemplar operação de Tratamento de Dados Pessoais com finalidade discriminatória, ilícita ou abusiva.
- **Responsabilização e Prestação de Contas:** O Projeto deverá contemplar a adoção de medidas capazes de evidenciar o atendimento à legislação e normas aplicáveis à proteção de Dados Pessoais.

Além do exposto acima, todos os Colaboradores deverão observar as demais Políticas de Proteção de Dados da ENGECOMP.

16.4. PROCEDIMENTOS INICIAIS PARA A AVALIAÇÃO DE UM PROJETO

Todos os Projetos da ENGECOMP que envolverem o Tratamento de Dados Pessoais precisarão ser avaliados sob o aspecto da privacidade e segurança dos Dados Pessoais, desde a concepção, durante toda a fase de desenvolvimento, até a execução de um novo produto ou serviço.

O Gestor responsável pelo Projeto deverá submetê-lo ao Encarregado de Proteção de Dados Pessoais, com a identificação do grau de exposição dos dados pessoais definida.

O Encarregado emitirá parecer sobre o Projeto e para a devida apreciação, ação de correção ou aprovação.

16.5. IDENTIFICAÇÃO DO GRAU DE EXPOSIÇÃO DOS DADOS PESSOAIS DO PROJETO

A escala a seguir se propõe a orientar essa classificação.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

Grau de Exposição	Responsável pela aprovação do projeto	Descrição do grau de exposição do dado pessoal
Muito baixo	Gestor da área ou responsável pelo compartilhamento	Quando há compartilhamento de Dados Pessoais Anonimizados ou estatísticos que não possibilitam a identificação de um Titular de Dados.
Baixo	Encarregado	Quando um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
Médio	Subcomissão de privacidade e Diretoria Executiva	Quando há o compartilhamento de Dados Pessoais sem qualquer procedimento para mascaramento ou vínculo direto com o titular.
Alto	Subcomissão de privacidade e Diretoria Executiva	Quando há compartilhamento de Dados Pessoais classificados como: (i) Dados Pessoais Sensíveis; (ii) Dados Pessoais de criança e adolescente; (iii) Dados Pessoais Financeiros; (iv) Dados Pessoais de Comportamento.
Muito alto	Subcomissão de privacidade e Diretoria Executiva	Quando há Compartilhamento/Transferência Internacional de Dados Pessoais.

16.6. LEGÍTIMO INTERESSE COMO BASE LEGAL DE TRATAMENTO DE DADOS PESSOAIS

Caso o Encarregado identifique o Legítimo Interesse como Base Legal cabível para o Tratamento pretendido este deverá emitir seu parecer e encaminhar os documentos ao responsável pela aprovação do Projeto.

16.7. PARECER DO ENCARREGADO PELO TRATAMENTO DOS DADOS PESSOAIS

O parecer a ser emitido pelo Encarregado deverá ser anexado ao relatório de classificação de grau de exposição e, caso aplicável, ao LIA. O parecer deve ser conclusivo no que se refere à adequação do Projeto às leis, normas, procedimentos e políticas internas da Companhia relativas à privacidade e proteção de Dados Pessoais, indicando claramente se o Projeto pode ser aprovado ou não, bem como as medidas a serem tomadas para a sua adequação, se necessário.

O Encarregado poderá solicitar informações adicionais sobre o Projeto e promover as diligências que entender necessárias para emitir o parecer.

A qualquer momento, o Encarregado poderá submeter a aprovação do Projeto a Subcomissão de Privacidade e Segurança, com as respectivas informações e seu parecer, independentemente do grau de exposição identificado, desde que justifique tal medida.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

16.8. CONTROLE E GESTÃO DO GRAU DE EXPOSIÇÃO DO DADO

A subcomissão de Privacidade, o Encarregado, o Gestor da Área responsável pelo Projeto, bem como o gestor do Projeto deverão controlar e/ou gerir os Projetos prestando especial atenção aos seguintes pontos:

- Qual a Base Legal das operações de Tratamento de dados no âmbito do Projeto?
- O Projeto envolve o Tratamento de Dados Pessoais Sensíveis?
- O Projeto envolve dados financeiros?
- O Projeto envolve dados que representam/revelam segredo de negócio?
- O Projeto envolve Dados Pessoais de Crianças?
- O Projeto envolve aquisição de dados de Terceiros?
- O Projeto envolve Compartilhamento de dados com Terceiros?
- O Projeto não envolve teste em ambiente controlado, Anonimização, Pseudonimização e/ou Eliminação de dados?
- Projeto envolve processo com decisões automatizadas?

A análise desses pontos deverá ser sempre suportada por assessoria jurídica especializada.

16.9. CONSIDERAÇÕES FINAIS

Para o esclarecimento de dúvidas, entre em contato pelo canal dpo@engecomp.com.br

O cumprimento desta Política é de suma importância e dever de todos. Em caso de não observância desta Política, favor reportar imediatamente ao Encarregado pela Proteção de Dados, pelo e-mail: dpo@engecomp.com.br

As denúncias de violações às Políticas e Procedimento serão anônimas e a não-retaliação será garantida.

16.10. EXCEÇÕES

Não se aplica.

16.11. DOCUMENTOS RELACIONADOS

- Política de Manuseio de Dados Pessoais;
- Política para Uso e Gestão do Consentimento;
- Código de Conduta.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

17. RESPONSABILIDADE DO ENCARREGADO DA PRIVACIDADE

17.1. OBJETIVO

Estabelecer a sistemática para a trabalho do Encarregado pela privacidade de dados junto a ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

17.2. CONTROLE DOS RISCOS

a) Garantir a constante atualização do registro de atividades de tratamento e respectivas bases legais.

b) Elaborar um Relatório de Impacto à Proteção de dados pessoais (“RIPD"), sempre que entender pertinente, independentemente da sensibilidade do Projeto/Serviço.

c) Aprovar o Relatório descrito no item “RELATÓRIO DE AVALIAÇÃO” nos casos de operações com níveis de exposição baixo e médio.

d) Emitir o parecer a respeito do Relatório descrito no item “RELATÓRIO DE AVALIAÇÃO nos casos de operações com níveis de exposição alto e muito alto.

e) Realizar o acompanhamento periódico/monitoramento das operações de compartilhamento, tomando as medidas necessárias para mitigar eventuais riscos identificados.

17.3. CONTROLES DOS INCIDENTE DE SEGURANÇA

a) Coordenar a resposta ao incidente.

b) Notificações e comunicações efetuadas sobre o incidente.

c) Assegurar que ocorra o menor tempo de reação entre a descoberta do incidente e o início do seu gerenciamento.

d) Identificar a causa raiz do incidente com o serviço de proteção de dados pessoais.

e) Medir o impacto financeiro, reputacional e operacional do incidente na Empresa.

17.4. CONTROLE DAS ATIVIDADES DE MANUSEIO DOS DADOS PESSOAIS

a) Manter o registro das operações de manuseio de dados pessoais, contemplando a respectiva base legal.

b) Analisar e aprovar ou reprovar as solicitações de suspensão de prazo de armazenamento de dados pessoais.

c) Analisar situações em que os dados pessoais de crianças poderão ser manuseados sem o consentimento de um dos pais ou responsável legal.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

17.5. CONTROLE DO COMPARTILHAMENTO DE DADOS COM TERCEIROS

Nas operações de compartilhamento de sensibilidade crítica, assegurar-se que:

a) O grau de proteção de dados pessoais do país destinatário tenha sido reconhecido pela ANPD como adequado ao previsto na legislação brasileira vigente.

b) O terceiro destinatário garanta o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados adotado pela legislação brasileira vigente.

c) Manter o registro das operações de compartilhamento com terceiros, contemplando a respectiva Base Legal e elaborar o Relatório de Impacto à Proteção de Dados Pessoais, quando entender necessário.

d) Garantir que as diligências prévias e necessárias ao compartilhamento de dados pessoais tenham sido observadas pela Área responsável pelo Compartilhamento.

e) Armazenar o registro relativo às diligências para o compartilhamento de dados pessoais, realizadas pela área responsável pelo compartilhamento.

17.6. GESTÃO DO CONSENTIMENTO

a) Monitorar periodicamente a atividade de tratamento baseada em consentimento, para garantir que não houve mudança na finalidade para a qual o titular deu seu consentimento.

b) Garantir que dados pessoais dos titulares que revogaram seu consentimento não sejam tratados sem que haja outra base legal que autorize o tratamento.

c) Garantir que a Empresa disponibilize método simplificado para que o titular possa, a qualquer momento, revogar o consentimento.

d) Aprovar as cláusulas/scripts de informação e requisição do consentimento.

e) Garantir que os registros relativos à obtenção e revogação do consentimento sejam armazenados e documentados de forma organizada.

f) Monitorar se as solicitações de revogação estão sendo devidamente respondidas e observadas pelos Terceiro.

17.7. NOVOS PROJETOS QUE ENVOLVAM DADOS DOS TITULARES

a) Emitir parecer sobre a viabilidade do projeto, do ponto de vista de privacidade e proteção de dados pessoais.

b) Verificar a adequação do tratamento à base legal do Legítimo Interesse.

c) Emitir o parecer de recomendação sobre a aprovação ou não de um projeto que envolva tratamento de dados pessoais, de forma clara e compreensível.

d) Executar as ações necessárias para a emissão do parecer.

e) Dar suporte, quando solicitado, ao gestor responsável pelo projeto.

f) Manter organizados e atualizados os registros do processo de aprovação dos projetos.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

g) Aprovar ou não os projetos, quando o gestor do projeto também for o gestor da área responsável pelo projeto.

17.8. SOBRE OS SERVIÇOS DO ESCRITÓRIO DE PRIVACIDADE

Ser o responsável principal pela entrega dos serviços do Catálogo de Serviços de Privacidade contemplando os seguintes serviços:

a) **Análise de contratos:** Análise de textos jurídicos que tratam de atividades que envolvem o tratamento de dados.

b) **Auditoria de Fornecedor e Parceiros:** Em cumprimento do mandamento legal e contratual a Empresa adota a boa prática de auditar o ambiente de TI e Privacidade de empresas que desempenham o papel de Operador dos dados dos Titulares de Dados Pessoais sob atenção da Empresa (Controlador).

c) **Ser auditado por cliente:** Nos contratos em que a Empresa desempenha o papel de Operador, o Controlador tem a prerrogativa de realizar auditoria no ambiente de TI e Privacidade do Operador. Diante de um evento dessa natureza existe uma série de ações que devem ser realizadas.

d) **Demanda interna:** Este serviço visa atender as diversas solicitações do negócio que não estão pré-definidas neste Catálogo de Serviços. Em geral, se referem a solicitações como treinamento, apoio em reuniões de negócio, participações em projetos etc.

e) **Analisar controle:** Os serviços organizados de TI ou negócio são estruturados por Controles associados a processos de trabalho. Alguns desses controles são declarados em Políticas ou Procedimentos Corporativos, outros são inerentes a sistemas que automatizam as tarefas de negócio. Podem ser relacionados a aplicação de leis, normas, contratos ou regimentos internos. A área de Privacidade pode ser acionada para analisar esses itens e propor ajustes, liberar o uso ou gerar algum parecer técnico.

f) **By Design (novo projeto):** Novos projetos devem ter suas atividades de tratamento de dados analisadas em tempo de projeto e antes da assinatura de contratos. Este serviço visa mitigar a exposição de riscos de privacidade.

g) **Dúvidas Operacionais:** Em geral, se referem a solicitações pontuais como dúvidas sobre como tratar dados pessoais, solicitações de suporte relativo ao uso e aplicação de instruções providas em contratos ou esclarecimento quanto a comportamento adequado nas operações cotidianas da Empresa.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

18. POLÍTICA DE GERENCIAMENTO DO CICLO DE VIDA DE DESENVOLVIMENTO DE SISTEMAS

18.1. OBJETIVO

Esta política define os princípios e diretrizes para o gerenciamento do ciclo de vida de desenvolvimento de sistemas (SDLC) junto a ENGECOMP Marketing ltda e suas controladas, coligadas e sob controle comum ("Empresa"). O objetivo é assegurar a entrega de sistemas de alta qualidade, confiáveis e seguros, que atendam às necessidades dos clientes e estejam em conformidade com as normas ISO 20000, ISO 15504 e ISO 29110.

18.2. TERMOS E DEFINIÇÕES

- Análise de Requisitos: Processo de coleta, análise e documentação das necessidades dos usuários e stakeholders, transformando-as em requisitos funcionais e não funcionais do sistema.
- Arquitetura de Software: Estrutura fundamental do sistema, definindo seus componentes, interfaces e interações.
- Caso de Uso: Descrição detalhada de como um usuário interage com o sistema para atingir um objetivo específico.
- Ciclo de Vida de Desenvolvimento de Sistemas (SDLC): Conjunto de fases e atividades que abrangem todo o processo de desenvolvimento de um sistema, desde a concepção até a obsolescência.
- Conformidade: Ação de estar em acordo com as normas, regulamentos e políticas aplicáveis.
- Controle de Versão: Sistema que gerencia as alterações feitas no código fonte e outros artefatos do projeto, permitindo o rastreamento e a reversão de versões.
- Desenvolvimento de Software: Processo de criação e implementação de software, incluindo codificação, testes e documentação.
- Documentação: Conjunto de documentos que descrevem o sistema, seus processos e resultados, incluindo requisitos, design, código fonte, planos de teste e manuais do usuário.
- Gerenciamento de Incidentes e Problemas: Processo de identificação, registro, análise e resolução de incidentes e problemas que afetam a operação do sistema.
- Integração Contínua: Prática de integrar e testar o código fonte com frequência, geralmente várias vezes ao dia, para detectar e corrigir erros precocemente.
- ISO 15504: Norma internacional que define um modelo para avaliação da maturidade dos processos de software.
- ISO 20000: Norma internacional que especifica os requisitos para um sistema de gestão de serviços de TI (SGSTI).
- ISO 29110: Norma internacional que fornece diretrizes para o desenvolvimento de software em pequenas e microEmpresas (PMEs).
- Manutenção de Software: Processo de modificação de um sistema de software após a entrega, para corrigir defeitos, melhorar o desempenho ou adaptar-se a novas necessidades.
- Melhoria Contínua: Processo de busca constante por oportunidades de aprimoramento nos processos e produtos.
- Plano de Implantação: Documento que descreve as etapas e os recursos necessários para implantar o sistema em ambiente de produção.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Plano de Projeto: Documento que define o escopo, os objetivos, os recursos, o cronograma e os riscos do projeto.
- Projeto de Software: Processo de definição da estrutura, design e interface do usuário do sistema.
- Requisitos Funcionais: Descrição das funcionalidades que o sistema deve realizar.
- Requisitos Não Funcionais: Descrição das características e qualidades do sistema, como desempenho, segurança e usabilidade.
- Segurança da Informação: Conjunto de medidas para proteger a confidencialidade, integridade e disponibilidade dos dados.
- Stakeholders: Pessoas ou organizações que têm interesse no projeto, como clientes, usuários, gerentes e desenvolvedores.
- Teste de Software: Processo de verificação e validação do software para garantir que ele atenda aos requisitos e funcione corretamente.
- Teste de Aceitação: Teste realizado pelos usuários finais para verificar se o sistema atende às suas necessidades e expectativas.
- Teste de Desempenho: Teste que avalia o desempenho do sistema em termos de velocidade, capacidade e estabilidade.
- Teste de Segurança: Teste que avalia a vulnerabilidade do sistema a ataques e acessos não autorizados.
- Teste de Usabilidade: Teste que avalia a facilidade de uso e a experiência do usuário com o sistema.
- Testes Unitários: Testes que verificam o funcionamento correto de cada componente individual do sistema.
- Validação: Processo de garantir que o sistema atenda às necessidades do usuário.
- Verificação: Processo de garantir que o sistema foi desenvolvido corretamente, de acordo com as especificações.

18.3. INTRODUÇÃO

Esta política tem por finalidade estabelecer os princípios, diretrizes e controles para o gerenciamento do ciclo de vida de desenvolvimento de sistemas na Empresa, visando a excelência na prestação de serviços e o contínuo aprimoramento dos processos de desenvolvimento. O documento abrange desde a concepção até a desativação dos sistemas, assegurando conformidade com as melhores práticas de gerenciamento e aderência aos padrões internacionais de qualidade, conforme estabelecido nas normas ISO 20000, ISO 15504 e ISO 29110.

Na Empresa a principal aplicação desses ditames são nos sistemas de gestão de relacionamento com titulares de dados e canal de denúncias, garantindo que os processos de desenvolvimento atendam não somente aos requisitos técnicos, mas também às demandas de governança, segurança e confiabilidade que caracterizam um ambiente regulado e competitivo.

Os principais objetivos desta política são:

- **Garantir a qualidade dos produtos e serviços de software**, por meio da padronização dos processos de desenvolvimento e da aplicação de controles internos que permitam a mensuração e a melhoria contínua.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Alinhar os processos de desenvolvimento com os requisitos das normas ISO 20000, ISO 15504 e ISO 29110**, promovendo a maturidade dos processos e a eficiência operacional.
- **Assegurar o atendimento aos requisitos de segurança, conformidade e governança corporativa**, fundamentais para a confiança dos clientes e a sustentabilidade dos negócios.
- **Facilitar a integração e a comunicação entre as áreas envolvidas no ciclo de vida do desenvolvimento**, promovendo um ambiente colaborativo e orientado para resultados.
- **Estabelecer critérios claros para a avaliação de riscos e oportunidades** em cada fase do desenvolvimento, permitindo a tomada de decisões informadas e a rápida adaptação a mudanças.

18.4. ESCOPO E APLICABILIDADE

Esta política se aplica a todos os projetos e atividades relacionados ao desenvolvimento, manutenção, operação e desativação de sistemas, englobando:

- **Planejamento e Concepção:** Definição de requisitos, análise de viabilidade técnica e econômica, e elaboração de planos de projeto.
- **Desenvolvimento e Teste:** Codificação, integração, testes unitários, de integração, de desempenho e de segurança, em conformidade com os requisitos estabelecidos.
- **Implantação e Operação:** Preparação para a liberação dos sistemas, suporte operacional e acompanhamento de incidentes, em alinhamento com as práticas de IT Service Management (ISO 20000).
- **Monitoramento e Melhoria Contínua:** Avaliação dos processos, realização de auditorias internas e externas, e implementação de ações corretivas e preventivas.
- **Desativação e Encerramento:** Processos de migração, backup e arquivamento dos sistemas, com o objetivo de garantir a preservação dos dados e a continuidade dos serviços.

Esta política deve ser observada por todas as áreas e colaboradores envolvidos no desenvolvimento e na manutenção dos sistemas, bem como por parceiros e fornecedores que atuem de forma integrada aos processos da organização.

18.5. PRINCÍPIOS E DIRETRIZES

18.5.1. CONFORMIDADE COM NORMAS E MELHORES PRÁTICAS

- **ISO 20000:** Os processos de suporte e operação dos sistemas deverão seguir os padrões de gerenciamento de serviços, garantindo a eficácia, a eficiência e a melhoria contínua do ambiente operacional.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **ISO 15504 (SPICE):** O desenvolvimento e a manutenção dos sistemas serão avaliados por meio de métricas de capacidade e maturidade de processos, visando identificar oportunidades de melhoria e promover a evolução contínua dos processos.
- **ISO 29110:** Para projetos em contextos de pequenas organizações ou equipes enxutas, os processos deverão ser simplificados, sem comprometer a qualidade, e alinhados com as diretrizes específicas para Very Small Entities (VSE).

Esta política se aplica a todos os projetos de desenvolvimento de sistemas na Empresa incluindo:

- Desenvolvimento de novos sistemas.
- Manutenção e evolução de sistemas existentes.
- Integração de sistemas.

18.5.2. PRINCÍPIOS GERAIS

- **Abordagem por Processos:** O desenvolvimento de sistemas será realizado com base em processos definidos e documentados, em conformidade com as normas ISO 20000, ISO 15504 e ISO 29110.
- **Foco no Cliente:** As necessidades e expectativas dos clientes serão priorizadas em todas as fases do SDLC.
- **Melhoria Contínua:** O processo de desenvolvimento de sistemas será continuamente avaliado e aprimorado.
- **Gestão de Riscos:** Os riscos serão identificados, avaliados e mitigados em todas as fases do SDLC.
- **Segurança da Informação:** A segurança da informação será integrada ao processo de desenvolvimento de sistemas, garantindo a confidencialidade, integridade e disponibilidade dos dados.

18.5.3. GERENCIAMENTO DO CICLO DE VIDA

Cada fase do ciclo de vida de desenvolvimento de sistemas deverá ser formalizada por meio de processos documentados, com atividades, entradas, saídas, responsáveis e critérios de aceitação definidos, conforme descrito abaixo:

- **Planejamento:**
    - Definição de escopo, objetivos, prazos e recursos necessários.
    - Identificação e análise dos riscos, com elaboração de planos de mitigação.
    - Estabelecimento dos critérios de qualidade e conformidade que orientarão as fases subsequentes.
- **Análise de Requisitos:**

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Coleta, análise e documentação dos requisitos do sistema, com base nas necessidades dos clientes e nas normas aplicáveis.
- Criação de casos de uso e cenários de testes.
- Validação dos requisitos com os stakeholders.

- **Projeto:**
  - Definição da arquitetura, design e interface do usuário do sistema.
  - Criação de protótipos e modelos de dados.
  - Definição de padrões de codificação e design.
- **Desenvolvimento:**
  - Aplicação de metodologias ágeis ou tradicionais, conforme a complexidade e a criticidade do projeto.
  - Codificação, testes unitários e integração dos componentes do sistema.
  - Utilização de ferramentas de controle de versão e integração contínua.
  - Realização de revisões de código.
  - Revisões periódicas de código e utilização de ferramentas de integração contínua para garantir a qualidade do software.
  - Realização de testes de unidade, integração, desempenho e segurança, com base em cenários predefinidos.
- **Teste:**
  - Realização de testes de software, incluindo testes funcionais, de desempenho, de segurança e de usabilidade.
  - Criação de planos de testes e relatórios de defeitos.
  - Realização de testes de aceitação com os usuários finais.
- **Implantação:**
  - Planejamento detalhado de rollout e migração, com a definição de planos de contingência.
  - Realização de treinamentos e capacitações para os usuários finais e equipes de suporte.
  - Comunicação clara e documentada de alterações e novas funcionalidades.
- **Operação e Suporte:**

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Monitoramento contínuo dos sistemas com indicadores de desempenho (KPIs) alinhados às metas de qualidade e disponibilidade.
- Gestão de incidentes e problemas com procedimentos bem definidos, permitindo a rápida resolução e a prevenção de recorrências.
- Revisão periódica dos processos operacionais, com a aplicação de lições aprendidas e ajustes necessários para melhoria contínua.

- **Desativação:**
  - Planejamento para a transição ou encerramento do sistema, incluindo a gestão de dados e a comunicação com os usuários.
  - Garantia de que os processos de backup e arquivamento estejam em conformidade com as políticas de segurança e privacidade.
  - Documentação final que permita a auditoria e o aprendizado para futuros projetos.

18.6. RESPONSABILIDADES E PAPÉIS

A estrutura organizacional para o gerenciamento do ciclo de vida de desenvolvimento deverá ser claramente definida, contemplando:

- **Gestor de Projetos:** Responsável pelo planejamento, execução e controle de cada projeto, garantindo o alinhamento com os objetivos estratégicos da Empresa.
- **Analista de Requisitos:** Responsável pela coleta, análise e documentação dos requisitos do sistema.
- **Arquiteto de Softwares:** Responsável pela definição da arquitetura e design do sistema.
- **Equipe de Desenvolvimento:** Responsável por implementar os requisitos técnicos e garantir a qualidade do software, seguindo as diretrizes definidas.
- **Gestor de Qualidade e Conformidade:** Responsável por monitorar o desempenho dos processos, realizar auditorias internas e assegurar que todas as atividades estejam em conformidade com as normas ISO 20000, ISO 15504 e ISO 29110.
- **Testador de Software:** Responsável pela realização dos testes de software.
- **Equipe de Operações e Suporte:** Responsável pela manutenção, monitoramento e suporte dos sistemas implantados, atuando de forma proativa na identificação e resolução de incidentes.
- **Gerente de Infraestrutura:** Responsável pela implantação e manutenção do sistema em ambiente de produção.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Gerente de Segurança da Informação:** Responsável por garantir a segurança da informação em todas as fases do SDLC.
- **Stakeholders:** Envolvidos na definição dos requisitos, validação dos resultados e acompanhamento do desempenho dos sistemas.
- **Alta Direção:** Responsável por prover os recursos necessários e garantir a conformidade com esta política.

18.7. REQUISITOS E CONTROLES DOS PROCESSOS

Para garantir a conformidade e a eficácia dos processos, deverão ser implementados controles e mecanismos de monitoramento, conforme segue:

- **Gestão de Mudanças:**
  - Todo o processo de alteração dos sistemas deverá ser realizado mediante análise de impacto e autorização formal.
  - Registro de todas as mudanças em um sistema de controle de versões e mudanças, com auditorias periódicas para validação dos registros.
- **Gestão de Riscos:**
  - Identificação, análise, tratamento e monitoramento dos riscos em todas as fases do ciclo de vida.
  - Utilização de matrizes de risco e planos de contingência para mitigar impactos e garantir a continuidade dos serviços.
- **Gestão da Qualidade:**
  - Definição de métricas de desempenho e indicadores-chave (KPIs) para monitorar a qualidade dos processos e dos produtos finais.
  - Revisões e auditorias periódicas com base nas diretrizes das normas ISO 15504 e ISO 29110, permitindo a mensuração da maturidade dos processos e a implementação de ações corretivas e preventivas.
- **Documentação e Registro:**
  - Manutenção de um repositório centralizado para toda a documentação dos processos, garantindo rastreabilidade, transparência e facilidade de acesso.
  - Atualização contínua dos registros de desenvolvimento, testes, implantação e operações, com base em revisões periódicas e feedback dos stakeholders.

18.8. MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA

O monitoramento dos processos será realizado por meio de indicadores e auditorias internas, com foco em identificar oportunidades de melhoria e assegurar a conformidade com os padrões internacionais. As atividades incluem:

- **Auditorias Periódicas:**
  - Realização de auditorias internas e, quando necessário, auditorias externas para avaliar a aderência dos processos aos requisitos das normas ISO 20000, ISO 15504 e ISO 29110.
  - Relatórios de auditoria que evidenciem as não conformidades, riscos identificados e propostas de melhoria.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Feedback e Revisão dos Processos:**
    - Coleta sistemática de feedback dos usuários, clientes e equipes envolvidas para identificar pontos de melhoria e promover ajustes nos processos.
    - Revisão semestral desta política e dos procedimentos associados, garantindo a atualização constante e a evolução em resposta às demandas do mercado e às mudanças regulatórias.
- **Capacitação e Treinamento:**
    - Programas contínuos de treinamento e desenvolvimento para as equipes, com o objetivo de disseminar as melhores práticas e garantir o conhecimento atualizado das normas e dos processos.
    - Avaliação de desempenho e capacitação técnica, garantindo que as equipes estejam aptas a implementar e operar os sistemas com excelência.

18.9. DOCUMENTAÇÃO

Todos os artefatos produzidos durante o SDLC serão documentados e mantidos em um repositório centralizado, incluindo:

- Plano de projeto.
- Documento de requisitos.
- Documento de design.
- Código fonte.
- Planos de teste e relatórios de defeitos.
- Manuais do usuário.

18.10. CONSIDERAÇÕES FINAIS E COMPROMETIMENTO

Esta política reflete o compromisso da Empresa com a excelência, a transparência e a melhoria contínua no desenvolvimento de sistemas, bem como com a conformidade com os padrões internacionais de qualidade e governança. Todos os colaboradores e parceiros deverão observar rigorosamente as diretrizes aqui estabelecidas, contribuindo para um ambiente de inovação, segurança e alto desempenho.

A alta direção se compromete a:

- **Garantir os recursos necessários** para a implementação e manutenção dos processos definidos.
- **Promover a cultura de melhoria contínua,** incentivando a comunicação e a colaboração entre as áreas.
- **Realizar revisões periódicas** desta política, ajustando os controles e procedimentos conforme as necessidades estratégicas e as atualizações normativas.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

Esta Política de Gerenciamento do Ciclo de Vida de Desenvolvimento de Sistemas constitui um instrumento essencial para a padronização dos processos e a promoção de uma cultura organizacional orientada à qualidade, segurança e inovação, estando em plena sintonia com as diretrizes e os conteúdos descritos no arquivo de referência.

Ao adotar esta política, a Empresa reforça sua posição no mercado, assegurando a confiabilidade e a qualidade dos serviços prestados aos clientes e garantindo a aderência plena aos requisitos das normas ISO 20000, ISO 15504 e ISO 29110.

19. POLÍTICA DE CONFORMIDADE LEGAL E NORMATIVA

19.1. OBJETIVO

Estabelecer a sistemática para a garantia da conformidade legal e normativa junto a ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente “Empresa”.

19.2. CONFORMIDADE COM REQUISITOS LEGAIS

Como parte do compromisso da Empresa com a conformidade legal e regulatória, é estabelecida uma rotina mensal de verificação e atualização dos requisitos legais aplicáveis ao negócio. O objetivo deste procedimento corporativo é garantir que novas leis e regulamentos sejam identificados e se estabeleça meios para se implementar as mudanças necessárias na operação da Empresa.

19.3. PROGRAMA DE CONFORMIDADE LEGAL E REGULATÓRIA

19.3.1. CONTEXTO LEGAL DA OPERAÇÃO DA EMPRESA

a) As seguintes leis são os ditames legais que definem as responsabilidades do negócio:
b) LGPD, Lei Geral de Proteção de Dados Pessoais –, lei nº 13.709, de 14 de agosto de 2018;
c) Lei nº 10.406 de 10 de janeiro de 2002 (Código Civil);
d) lei nº 9.609, de 19 de fevereiro de 1998 (Propriedade intelectual de programa de computado);
e) lei nº 9.279, de 14 de maio de 1996 (Propriedade industrial);
f) lei nº 9.610, de 19 de fevereiro de 1998 (Direitos autorais);
g) Lei 12.965/2014, (Marco Civil da Internet)
h) Código Penal, art. 151, 152, 154, 154-A, 298, 307, 207, 184p3, 266.
i) Lei nº 9.296/96, art. 10 (Lei das Interceptações Telefônicas);
j) Lei 7.492/86 art 18 (violação do sigilo de operações)
k) Lei 12.846/2013 (Lei Anticorrupção)
l) Lei 8.069/90 (Estatuto da Criança e do Adolescente)
m) Lei 12.853/2013 (Lei dos direitos autorais)

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

n) Lei 9.605/98 (Lei de crimes ambientais)
o) Lei 8.078/90 (Código do Consumidor)

19.3.2. CONTEXTO REGULATÓRIO DA OPERAÇÃO DA EMPRESA

a) ABNT NBR ISO_IEC_20000
b) ABNT NBR ISO_IEC_27000
c) ABNT NBR ISO_IEC_31.000
d) Framework COBIT
e) Framework ITIL

19.4. FLUXO DE TRABALHO PARA CONFORMIDADE

O seguinte fluxo de trabalho deve ser realizado para a garantia da conformidade na Empresa.

19.4.1. PARAMETRIZAÇÃO DA FERRAMENTA DE AUTOMAÇÃO

O Sistema de Gestão de Serviços de TI licenciado para a ENGECOMP deverá ser usado para o devido controle do workflow de conformidade.

Para controlar o **workflow de verificação de novas leis ou normas** que podem impactar a empresa, os seguintes campos são implementados para garantir o acompanhamento eficaz e completo:

19.4.2. CAMPOS PARA CONTROLE DO WORKFLOW

1. **Identificação**
   - **ID da Demanda:** Número único ou código identificador.
   - **Tipo de Norma:** Especificar se é uma lei, decreto, regulamentação, norma técnica, ou outro tipo de exigência.
2. **Informações Gerais**
   - **Título da Norma/Lei:** Nome ou descrição oficial.
   - **Descrição:** Breve resumo da norma ou lei e seu impacto potencial.
   - **Órgão Emissor:** Identificar a entidade responsável pela publicação ou regulamentação (e.g., Anvisa, Receita Federal, LGPD).
3. **Status**
   - **Status Atual:** Exemplos de status podem incluir:
     - Pendente de análise
     - Em avaliação de impacto
     - Implementação em andamento
     - Concluído

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **Prioridade:** Alta, Média ou Baixa, conforme o impacto ou prazo.

4. **Impacto e Avaliação**
   - **Área Impactada:** Identificar quais departamentos ou áreas da empresa serão afetados.
   - **Descrição do Impacto:** Detalhar os potenciais riscos ou ajustes necessários.
   - **Necessidade de Ajuste em Políticas:** Indicar se políticas ou procedimentos internos precisarão de alterações.
5. **Responsabilidades**
   - **Responsável pela Análise:** Nome ou equipe responsável pela análise da norma.
   - **Responsável pela Implementação:** Pessoa ou área que executará as mudanças necessárias.
6. **Datas e Prazos**
   - **Data de Publicação da Norma:** Data oficial da emissão ou atualização.
   - **Prazo para Conformidade:** Prazo legal para adequação à norma.
   - **Data de Última Revisão:** Atualização mais recente da análise ou status.
7. **Ações e Monitoramento**
   - **Plano de Ação:** Resumo das ações a serem realizadas para atender à norma.
   - **Status das Ações:** Detalhamento do progresso de cada tarefa associada.
   - **Comentários e Observações:** Notas adicionais sobre o progresso ou desafios.
8. **Evidências e Documentação**
   - **Documentos Relacionados:** Links ou referências a documentos associados (e.g., texto completo da norma, pareceres jurídicos).
   - **Evidências de Conformidade:** Registro de ações realizadas para atender aos requisitos.
9. **Auditoria e Avaliação**
   - **Revisão pelo Compliance:** Indicar se a conformidade foi validada pela equipe de SIPD.
   - **Resultado da Auditoria:** Registro de possíveis apontamentos ou ajustes recomendados após auditoria.
10. **Notificações**

- **Comunicações Realizadas:** Registro de notificações enviadas às áreas impactadas.
- **Treinamentos Necessários:** Indicar se foram realizados treinamentos associados à norma.

19.5. RESPONSABILIDADES

Equipe Jurídica e SIPD

- Monitorar as mudanças legais e regulamentares, além de orientar a equipe de segurança da informação sobre os impactos.

SIPD

- Abrir um evento no sistema de gestão de serviços de TI para iniciar o fluxo de verificação de novas leis e normas.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- Implementar controles para atender aos requisitos legais relacionados à proteção de dados e cibersegurança.
- Garantir que as atividades estejam alinhadas com a política e que os registros sejam mantidos adequadamente.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

20. POLÍTICA DE TRABALHO FORA DO ESCRITÓRIO (HOME-OFFICE)

20.1. INTRODUÇÃO

A presente Política de Trabalho Fora do Escritório (Home-Office) da ENGECOMP Consultoria e Locação de Sistemas LTDA que compreende doravante a marca ENGECOMP ou simplesmente "Empresa", foi desenvolvida para formalizar e orientar a prática do trabalho remoto na organização. Este documento estabelece as diretrizes, responsabilidades e procedimentos que devem ser seguidos por todos os prestadores de serviços que atuam nesta modalidade, garantindo a continuidade das operações, a segurança da informação, a conformidade legal e o bem-estar dos nossos profissionais. A adoção do trabalho remoto reflete o compromisso da ENGECOMP com a modernização das relações de trabalho e a busca por um modelo que concilie produtividade, flexibilidade e qualidade de vida, em alinhamento com os valores e a cultura da empresa.

20.2. OBJETIVO

O objetivo desta política é definir as regras e os padrões para a execução do trabalho em regime de home-office na ENGECOMP. Busca-se assegurar que as atividades laborais realizadas fora das dependências da empresa mantenham o nível de segurança, qualidade, eficiência e conformidade exigido nas operações presenciais. Adicionalmente, a política visa a orientar sobre o uso adequado dos recursos de tecnologia da informação, proteger os dados corporativos e de clientes, e estabelecer um ambiente de trabalho remoto que seja produtivo, seguro e saudável para todos os envolvidos.

20.3. ABRANGÊNCIA

Esta política aplica-se a todos os prestadores de serviços da ENGECOMP e suas controladas, em todos os níveis hierárquicos, que estejam autorizados a realizar suas atividades profissionais em regime de trabalho remoto, seja de forma integral, parcial ou em situações excepcionais.

20.4. DEFINIÇÕES

Para os fins desta política, os termos a seguir são definidos em conformidade com as normativas internas da ENGECOMP, especialmente a Política de Uso de Recursos de TI (PRTI V1) e o Procedimento Corporativo para Gestão da Segurança da Informação (PCSEG V1.0):

- **Trabalho Remoto (Home-Office):** Atividade laboral realizada preponderante ou totalmente fora das dependências físicas da empresa, com a utilização de tecnologias de informação e comunicação.
- **Ambiente de Trabalho Remoto:** Espaço físico, localizado na residência do prestador de serviço ou em outro local previamente acordado, a partir do qual as atividades profissionais são executadas.
- **Recursos de TI:** Conjunto de ativos de tecnologia mantidos ou operados pela ENGECOMP, como computadores, dispositivos móveis, softwares, sistemas, redes e serviços de comunicação.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

- **VPN (Virtual Private Network):** Rede privada virtual que estabelece uma conexão segura entre o dispositivo do prestador de serviço e a rede corporativa da ENGECOMP, sendo de uso obrigatório para acesso a sistemas internos.
- **Dado Pessoal:** Qualquer informação relacionada a uma pessoa natural identificada ou identificável, conforme definido pela Lei Geral de Proteção de Dados (LGPD).
- **Informação Confidencial:** Dados estratégicos, financeiros, técnicos, comerciais, de clientes, fornecedores ou prestadores de serviços, cujo acesso é restrito e cuja divulgação não autorizada pode causar prejuízos à empresa ou a terceiros.
- **Incidente de Segurança:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou à proteção de dados.

20.5. DIRETRIZES GERAIS

20.5.1. ELEGIBILIDADE E MODALIDADES DE TRABALHO REMOTO

A elegibilidade para o trabalho remoto será determinada pela natureza das atividades desempenhadas pelo prestador de serviço, pela necessidade operacional do departamento e pela avaliação do gestor direto. A ENGECOMP poderá adotar diferentes modalidades de trabalho remoto, como o regime integral (todos os dias da semana), parcial (híbrido, com alternância entre dias no escritório e dias remotos) ou excepcional (em situações pontuais e autorizadas). A modalidade aplicável a cada prestador de serviço será formalizada por meio de um aditivo contratual, que especificará as condições do regime de trabalho.

20.5.2. AMBIENTE DE TRABALHO E ERGONOMIA

É responsabilidade do prestador de serviço garantir que seu ambiente de trabalho remoto seja seguro, organizado e livre de distrações que possam comprometer a produtividade e a confidencialidade das informações. O espaço deve ser ergonomicamente adequado visando a preservar a saúde e o bem-estar do profissional.

20.5.3. JORNADA DE TRABALHO E CONTROLE DE PONTO

A jornada de trabalho em regime de home-office seguirá o que foi estabelecido no contrato de trabalho do prestador de serviço.

20.5.4. SEGURANÇA DA INFORMAÇÃO E DE DADOS

A segurança da informação é um pilar fundamental do trabalho remoto na ENGECOMP. Todos os prestadores de serviços devem seguir rigorosamente as diretrizes estabelecidas na Política de Segurança da Informação (PSI) e nos procedimentos corporativos relacionados, a fim de garantir a integridade, a confidencialidade e a disponibilidade dos dados da empresa e de seus clientes.

20.5.5. CONTROLE DE ACESSO E AUTENTICAÇÃO

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

O acesso aos sistemas e recursos de TI da ENGECOMP a partir de redes externas deve ser realizado exclusivamente por meio da VPN corporativa e Sharepoint. A autenticação em todos os sistemas críticos exigirá o uso de múltiplos fatores de autenticação (MFA). As senhas de acesso são pessoais, intransferíveis e devem seguir os padrões de complexidade definidos na Política de Uso de Recursos de TI, sendo trocadas periodicamente.

20.5.6. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

O manuseio de dados pessoais e informações confidenciais em ambiente de home-office deve seguir as mesmas regras de sigilo e proteção aplicadas no ambiente corporativo, conforme o Procedimento Corporativo para Manuseio de Dados Pessoais. É vedado o armazenamento de dados corporativos em dispositivos de armazenamento pessoal (pen drives, HDs externos) não autorizados. Documentos físicos que contenham informações sensíveis devem ser manuseados com o máximo de cuidado e descartados de forma segura.

20.5.7. USO DE EQUIPAMENTOS E DISPOSITIVOS

Os prestadores de serviços em regime de home-office deverão, preferencialmente, utilizar os equipamentos de TI (notebooks, etc.) fornecidos pela ENGECOMP. Tais equipamentos são de uso exclusivo para atividades profissionais e são configurados com todas as ferramentas de segurança necessárias (antivírus, firewall, etc.). O uso de dispositivos pessoais (BYOD - Bring Your Own Device) para acessar informações corporativas só será permitido em casos excepcionais, mediante autorização e com a instalação dos softwares de segurança exigidos pela empresa.

20.5.8. CONECTIVIDADE E REDES SEGURAS

O prestador de serviço é responsável por prover uma conexão de internet estável e segura para a realização de suas atividades. A rede Wi-Fi doméstica utilizada para o trabalho deve ser protegida por senha forte e, sempre que possível, configurada com o protocolo de segurança WPA2 ou superior. O uso de redes Wi-Fi públicas e não seguras para o acesso a sistemas corporativos é estritamente proibido.

20.6. COMUNICAÇÃO E COLABORAÇÃO

A manutenção de uma comunicação clara e eficiente é vital para o sucesso do trabalho remoto. Todos os prestadores de serviços devem aderir aos padrões de comunicação da ENGECOMP, garantindo a colaboração e o alinhamento entre as equipes.

20.6.1. CANAIS DE COMUNICAÇÃO OFICIAIS

O e-mail corporativo é a ferramenta principal para comunicações formais. Para interações em tempo real, como reuniões e discussões de equipe, devem ser utilizadas as plataformas de videoconferência e mensageria instantânea homologadas pela ENGECOMP. Conforme o "Procedimento Corporativo para Uso de E-Mail e Mensagens Eletrônicas", o uso dessas ferramentas é estritamente profissional, e todas as comunicações estão sujeitas a monitoramento.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

20.6.2. REUNIÕES E INTERAÇÃO COM A EQUIPE

Os prestadores de serviços em home-office devem manter a disponibilidade para participar de reuniões virtuais e outras interações com a equipe durante o horário de trabalho. A frequência e o formato das reuniões de equipe serão definidos por cada gestor.

20.6.3. USO DE REDES SOCIAIS E IMAGEM CORPORATIVA

As diretrizes sobre o uso de redes sociais, estabelecidas no Código de Conduta, aplicam-se integralmente ao trabalho remoto. É proibida a divulgação de informações confidenciais ou estratégicas da ENGECOMP e de seus clientes. Os prestadores de serviços devem zelar pela imagem da empresa em todas as suas interações online, evitando associar opiniões pessoais à marca ENGECOMP sem autorização expressa.

20.7. RECURSOS E SUPORTE DE TI

A ENGECOMP garantirá os recursos tecnológicos necessários para a execução do trabalho remoto e prestará o devido suporte técnico para manter a produtividade e a segurança das operações.

20.7.1. FORNECIMENTO E MANUTENÇÃO DE EQUIPAMENTOS

Conforme a Política de Uso de Recursos de TI, a ENGECOMP poderá fornecer os equipamentos necessários (como notebooks e periféricos) para a realização do trabalho remoto. O prestador de serviço é responsável por zelar pela integridade e pelo bom funcionamento desses ativos. Qualquer defeito, dano, perda ou roubo do equipamento deve ser comunicado imediatamente ao departamento de TI.

20.7.2. SOFTWARE E LICENCIAMENTO

Todos os softwares necessários para a execução das atividades poderão ser fornecidos e licenciados pela ENGECOMP. É estritamente proibida a instalação de softwares não autorizados ou de origem duvidosa nos equipamentos da empresa. A área de TI é responsável por manter os sistemas e aplicativos atualizados com as últimas versões e correções de segurança.

20.7.3. SUPORTE TÉCNICO REMOTO

A ENGECOMP disponibilizará canais de suporte técnico para auxiliar os prestadores de serviços em home-office com questões relacionadas a hardware, software, conectividade e segurança. O atendimento será realizado de forma remota, e o prestador de serviço deverá garantir o acesso do técnico ao equipamento, quando necessário, para a solução de problemas.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

20.8. SAÚDE, SEGURANÇA E BEM-ESTAR

A ENGECOMP preza pela saúde e pelo bem-estar de seus prestadores de serviços, independentemente da modalidade de trabalho. As diretrizes a seguir visam a promover um ambiente de trabalho remoto seguro e saudável.

20.8.1. ERGONOMIA E SAÚDE OCUPACIONAL

O prestador de serviço deve seguir as orientações de ergonomia para prevenir lesões e problemas de saúde decorrentes da má postura ou de condições inadequadas de trabalho. É fundamental que o prestador de serviço realize pausas regulares e se atente aos sinais de desconforto físico, comunicando ao seu gestor e ao RH qualquer necessidade de ajuste.

20.8.2. EQUILÍBRIO ENTRE VIDA PESSOAL E PROFISSIONAL

A ENGECOMP incentiva o equilíbrio saudável entre as responsabilidades profissionais e a vida pessoal. É fundamental que os prestadores de serviços respeitem a jornada de trabalho contratual, incluindo os horários de início, término e pausas. A empresa promove o direito à desconexão, e os gestores devem evitar o contato com os prestadores de serviços fora do horário de expediente, exceto em situações emergenciais.

20.9. CONFORMIDADE E RESPONSABILIDADES

O cumprimento desta política é mandatório para todos os participantes do regime de trabalho remoto. O não cumprimento das diretrizes aqui estabelecidas sujeitará o infrator às medidas disciplinares cabíveis.

20.9.1. RESPONSABILIDADES DO PRESTADOR DE SERVIÇO

a) Cumprir a jornada de trabalho.
b) Manter um ambiente de trabalho remoto seguro, organizado e ergonômico.
c) Zelar pela segurança das informações e dos ativos de TI da empresa.
d) Utilizar os recursos de TI exclusivamente para fins profissionais.
e) Manter a comunicação com a equipe e o gestor de forma proativa.
f) Reportar imediatamente qualquer incidente de segurança, acidente de trabalho ou problema com os equipamentos.
g) Cumprir todas as políticas e procedimentos da ENGECOMP.

20.9.2. RESPONSABILIDADES DA ENGECOMP

a) Fornecer os recursos de TI necessários para a execução do trabalho remoto.
b) Oferecer suporte técnico, orientações sobre segurança da informação e ergonomia.
c) Respeitar a privacidade do prestador de serviço, limitando o monitoramento ao estritamente necessário para a segurança e a gestão do trabalho.
d) Manter canais de comunicação abertos para o suporte ao prestador de serviço.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

20.9.3. MONITORAMENTO, AUDITORIA E AÇÕES DISCIPLINARES

Conforme a Política de Uso de Recursos de TI, a ENGECOMP reserva-se o direito de monitorar o uso de seus sistemas e redes para garantir a segurança e a conformidade. A violação de qualquer uma das diretrizes desta política ou das demais normas da empresa será tratada de acordo com o estabelecido no Código de Conduta e na legislação vigente, podendo resultar em sanções que vão desde advertências até a rescisão do contrato de trabalho por justa causa.

20.10. DISPOSIÇÕES FINAIS

Esta política será revisada periodicamente para garantir sua adequação às mudanças na legislação, na tecnologia e nas necessidades da organização. Dúvidas e casos omissos serão tratados pelo departamento de Recursos Humanos em conjunto com a área de Segurança da Informação e o gestor do prestador de serviço.

20.11. REFERÊNCIAS

Esta política foi elaborada com base nos seguintes documentos e normativas da ENGECOMP:

- ENGECOMP - Código de Conduta Empresarial
- ENGECOMP - Política de Segurança da Informação (PSI)
- ENGECOMP - Procedimento Corporativo para Gestão da Segurança da Informação (PCSEG V1.0)
- ENGECOMP - Procedimento Corporativo para Manuseio de Dados Pessoais
- ENGECOMP - Política de Uso de Recursos de TI (PRTI V1)
- ENGECOMP - Procedimento Corporativo para Uso de E-Mail e Mensagens Eletrônicas
- Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018)
- ISO/IEC 27.000;
- ISO/IEC 20.000;
- ISO/IEC 31.000;

20.12. PENALIDADES

É exigido que todos os Usuários da Empresa o cumprimento desta política, constituindo violação a não observância dos preceitos nela descritos, podendo acarretar na aplicação de medidas disciplinares tais como advertência verbal, escrita e até mesmo em desligamento por justa causa, dependendo da gravidade da falta cometida aos Usuários próprios e ainda, penalidades contratuais aos Usuários terceiros, prestadores de serviços ou clientes que descumpram as regras contidas na política de segurança da informação.

Toda infração será avaliada pela área de SIPD, Gestão de Pessoas e Dep. Jurídico, através da instauração de sindicância interna e apuração do ocorrido e na sequência as medidas legais serão devidamente tomadas em face aos envolvidos.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

21. GLOSSÁRIO

AGENTES DE TRATAMENTO: O Controlador e o Operador de Dados Pessoais.

ANONIMIZAÇÃO: Processo pelo qual um dado relativo ao Titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

APROVADOR: Pessoa formalmente autorizada pelo gestor da informação para aprovação da concessão de acessos;

ÁREAS CUSTODIANTES: Áreas delegadas pelos gestores das informações "I/O - Information Owners" que, por definição da Empresa, tem autonomia em relação ao ciclo de vida de aquisição, desenvolvimento e manutenção dos sistemas;

ARTEFATOS CORPORATIVOS: Produtos, serviços, processos, práticas de negócio ou sistemas.

ATIVO DE INFORMAÇÃO: Toda informação, não importando a mídia que a suporte e que represente valor para os negócios da ENGECOMP;

AUTENTICIDADE: Propriedade da informação que confirma a originalidade de seu conteúdo, comprovando sua origem e sua autoria;

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD"): Órgão pertencente à administração pública federal, responsável pela fiscalização do cumprimento das disposições da Lei Geral de Proteção de Dados.

BYOD (BRING YOUR OWN DEVICE): Conceito que permite o uso de dispositivos móveis pessoais para exercer suas atividades no ambiente de trabalho conforme normas e requisitos estabelecidos pela empresa;

CLOUD COMPUTING: Computação (sistemas, banco de dados, aplicação, etc.) em nuvem, ou seja, é a entrega de serviços de TI onde o acesso é possível através de qualquer dispositivo, estando dentro ou fora da rede da empresa e empregando a internet como meio de comunicação;

COLABORADOR (ES): São todos os empregados e funcionários da ENGECOMP, incluindo conselheiros e diretores.

COMITÊ DE PRIVACIDADE: Grupo de pessoas, composto pelo Encarregado, responsável por tomar as decisões relativas a Projetos classificados com alto Nível de Sensibilidade.

CONFIDENCIALIDADE: Propriedade da informação que garante que o conteúdo é acessível somente por pessoas autorizadas;

CONFLITO DE INTERESSES: Situações nas quais a atuação do funcionário ou Fornecedor indica a busca de quaisquer vantagens e/ou benefícios próprios ou de terceiros, em detrimento dos interesses da empresa;

CONSENTIMENTO: Manifestação livre, informada e inequívoca do titular que autoriza o tratamento dos seus dados pessoais para uma finalidade específica.

Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

CONTAS / LOGIN: Identificação de um usuário na rede corporativa, aplicativos ou outros recursos de processamento de informações;

CONTROLADOR: Parte que determina as finalidades e os meios de Tratamento de Dados pessoais;

DADOS ANONIMIZADOS: Dados objeto de utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

DADOS COMPORTAMENTAIS: Dados Pessoais que demonstrem ou revelem o comportamento do Titular. Exemplos: Dados de localização, consumo, hábitos, preferências, endereço IP, cookies, logs de conexão, logs de acesso.

DADOS FINANCEIROS: Dados Pessoais que remetam ou revelem qualquer aspecto financeiro do Titular. Exemplos: número de conta, cartão de crédito, senha, código verificador, renda, salário, benefícios.

DADOS PESSOAIS: Quaisquer informações relativas a uma pessoa singular identificada ou identificável; é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, Dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

DADOS PESSOAIS SENSÍVEIS: Dados Pessoais sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde, ou à vida sexual, Dado genético ou biométrico, quando vinculados a uma pessoa natural.

DAR: Documento de Aceitação de Riscos, utilizado para formalizar os riscos de determinado projeto ou situação;

DISPONIBILIDADE: Propriedade da informação que garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

ENCARREGADO: Pessoa indicada pelo Controlador e operador para atuar como canal de comunicação entre o Controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD).

FINALIDADE: Motivo pelo qual o dado pessoal será tratado, ou objetivo que se pretende atingir com o tratamento dos dados.

FORNECEDOR: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços à empresa, necessários e utilizados na execução do objeto social da empresa;

FRAUDE: Subterfúgio para alcançar um fim ilícito e/ou engano dolosamente provocado, induzimento ao erro ou aproveitamento de preexistente erro alheio;

GESTOR DA ÁREA: Pessoa designada pela ENGECOMP para gerir uma determinada área dentro da sua estrutura.

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

GESTOR DA INFORMAÇÃO ("INFORMATION OWNERS"): Diretores ou níveis hierárquicos acima, responsáveis pelas informações geradas e/ou manuseadas para realização dos processos de negócio da ENGECOMP;

GESTOR DE ACESSOS: Pessoa formalmente nomeada para apoio na implementação das regras de aprovação e concessão de acessos;

GESTOR DO PROJETO: Colaborador designado pela ENGECOMP para gerir um Projeto e que será responsável pela resposta do Questionário de Avaliação de Sensibilidade.

INCIDENTE DE SEGURANÇA DE INFORMAÇÕES: Qualquer evento que afete ou possa afetar, de forma prejudicial e/ou maliciosa, os negócios e/ou a integridade física e/ou lógica dos ambientes da ENGECOMP;

INCIDENTES: Acesso, aquisição, uso, compartilhamento, destruição, alteração ou indisponibilidade de Dados Pessoais, proposital ou acidental, não autorizada ou ilícita. Violação da confidencialidade, integridade e disponibilidade de Dados Pessoais. Exemplos: Perda de laptop com Dados pessoais de colaboradores, que não estejam criptografados; Envio de e-mail que contenha Dados pessoais de clientes, para o destinatário errado; Arquivo de currículos de candidatos a uma vaga exposto em um diretório aberto na internet, com acesso sem necessidade de identificação (usuário e senha); Extração de Dados pessoais de servidores da empresa por um terceiro que utilize de falhas técnicas e engenharia social ("ataque hacker").

INFORMAÇÕES CORPORATIVAS: Informações direta ou indiretamente envolvidas na operação dos sistemas corporativos da ENGECOMP, independentemente do local onde tenham sido produzidas;

INFORMATION OWNER: Responsável (gestor) das informações de um sistema ou módulo do sistema;

INTEGRIDADE: Propriedade da informação que garante a salvaguarda da exatidão e completude da informação;

LEGALIDADE: Propriedade que garante que a informação se encontra em concordância com as legislações vigentes e aplicáveis a ENGECOMP;

MATERIAIS, BENS E SERVIÇOS: Qualquer bem, móvel ou imóvel, material ou imaterial, assim como qualquer atividade fornecida mediante remuneração, que são adquiridos pela ENGECOMP ;

MESA LIMPA: Prática na qual, ao final do expediente, os documentos considerados confidenciais ou uso interno são armazenados em locais seguros, tais como: armário e gavetas disponíveis com chaves;

NÃO REPÚDIO: Propriedade da informação em que o autor não pode negar a responsabilidade sobre ele atribuída. Consegue-se estabelecer a característica de não repúdio com a combinação de confidencialidade e integridade da informação;

OWASP (OPEN WEB APPLICATION SECURITY PROJECT): Entidade dedicada a capacitar organizações para conceber, desenvolver, adquirir, operar e manter aplicações que precisam ser confiáveis para desenvolvimento de aplicações *web*;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

PERFIL DE ACESSO: Conjunto de permissões definidas em um sistema ou aplicativo focado nas necessidades de um determinado posto de trabalho ou cargo seguindo as necessidades do negócio;

PROJETO: Toda e qualquer atividade e/ou iniciativa para concepção, desenvolvimento e/ou atualização de novos produtos ou serviços de interesse da ENGECOMP.

PSEUDONIMIZAÇÃO: É o Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional, mantida separada pelo Controlador em ambiente controlado e seguro.

QUESTIONÁRIO DE AVALIAÇÃO DE RISCO: Documento com perguntas elaboradas e estruturadas para extrair respostas que revelem informações relacionadas às operações de Tratamento de Dados Pessoais no Projeto, de modo a permitir a avaliação e classificação do Nível de Risco. Objeto do Anexo I.

QUESTIONÁRIO DE LEGÍTIMO INTERESSE ("LIA"): Documento com perguntas elaboradas e estruturadas para extrair respostas que revelem informações relacionadas à utilização do Legítimo Interesse como base legal de Tratamento de Dados Pessoais no Projeto. Objeto do Anexo II.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: Documentação do controlador que contém a descrição dos processos de tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

REQUISITANTE: Responsável por emitir a requisição de compras necessária para solicitar a contratação de um material ou serviço.

SEGREGAÇÃO DE FUNÇÕES: Princípio básico de controle que consiste na separação de funções, normalmente de autorização, aprovação, execução e controle, de tal forma que nenhuma pessoa, pelo acúmulo de privilégios, detenha competências em desacordo com este princípio;

SEGURANÇA DA INFORMAÇÃO: Conjunto de medidas que visam a preservação da confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações;

SEGURANÇA FÍSICA E PATRIMONIAL: Conjunto de medidas que têm por objetivo a proteção contra ocorrências, visando evitar, conter e/ou minimizar atos deliberados que possam ou não causar danos às pessoas, ao patrimônio, às informações, à execução dos serviços ou à imagem da ENGECOMP;

SENHA FORTE: Conjunto de caracteres recomendados que, quando da verificação da identidade de um usuário, gera maior segurança e proteção contra *hackers, softwares* maliciosos etc.;

SIPD: Equipe responsável pela gestão dos serviços e ativos relativos a Segurança da Informação e Privacidade de Dados.

SISTEMA DE CONTROLE DE ACESSO: Sistema de controle que garante que os acessos sejam efetuados apenas por pessoas autorizadas;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados

O PRESENTE DOCUMENTO FOI ELABORADO DE ACORDO COM O CÓDIGO DE ÉTICA DA ENGECOMP

SISTEMA DE INFORMAÇÃO: Conjunto de informações relacionadas, de modo a formar uma base de conhecimento sobre um processo, suportada ou não por programas de computador;

SYSTEM OWNER DE INFRA/APLICAÇÃO: Responsável técnico pelo funcionamento do sistema/aplicação;

TERCEIROS: São todos os prestadores de serviços, trabalhadores terceirizados, parceiros comerciais, fornecedores e representantes da ENGECOMP.

TESTES DE SEGURANÇA: Testes a serem aplicados aos sistemas de informação visando à validação sobre o atendimento dos requerimentos de segurança;

TITULAR DOS DADOS: Pessoa natural a quem se referem os Dados Pessoais objeto de Tratamento pela ENGECOMP.

TRATAMENTO: Qualquer operação ou conjunto de operações efetuadas com Dados Pessoais ou sobre conjuntos de Dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição

USERNAME: Chave única de identificação do usuário para acesso à rede, correio eletrônico e sistemas também conhecido como *login*.

USO COMPARTILHADO DE DADOS: Comunicação, difusão, transferência internacional, interconexão de Dados Pessoais ou tratamento compartilhado de bancos de Dados Pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

USUÁRIO DA INFORMAÇÃO: Pessoa que tem como papel, utilizar-se das informações da ENGECOMP no desempenho de suas atividades e em conformidade com a política e normas de segurança da informação;

ENGECOMP CONSULTORIA E LOCACAO DE SISTEMAS LTDA
Todos os Direitos Reservados