

# PROPOSTA COMERCIAL

Daniel Henrique dos Santos Rodrigues  
Luiz Felipe Rosa Moura  
Maicon Wansley Antunes da Silva  
Vitor Almeida da Silva  
Yuri Gabriel Jales da Silva

## IMPLEMENTAÇÃO DE SGSI

PROF. JÚLIO ALBERTO VANSAN GONÇALVES

**CLIENTE:** TechPro - Fabricante de componentes industriais

**PROPOSTA N°:** B23FYA12-v1

**DATA DE EMISSÃO:** 05/04/2024



**Desenvolvendo o futuro tecnológico da sua empresa**

Somos uma empresa que oferece produtos e serviços de tecnologia com um portfólio diversificado de ofertas para a solução ideal com propostas complementares e flexíveis.

Pertencente ao grupo empresarial CONSUTECH, há mais de 20 anos no mercado, conectamos ideias a um mundo de possibilidades tecnológicas, garantindo eficiência operacional, qualidade técnica e foco em pessoas.

**EFICIÊNCIA OPERACIONAL,  
QUALIDADE TÉCNICA,  
FOCO EM PESSOAS.**



## **TIPOS DE SERVIÇO**

- Implementação de SGSI
- Infraestrutura
- Suporte técnico
- Segurança
- Monitoramento
- Servidores

## **PRODUTOS**

- Firewall
- Switch, Access Point
- Antivírus, AntiSpam, WAF, Backup
- PABX Virtual (VoIP)
- Licenciamento Microsoft
- Cloud (AWS, GCP, AZURE)
- Servidor, Notebook, Desktop, Impressoras
- Cabeamento Estruturado e CFTV

## À: PROTECH - FABRICANTE DE COMPONENTES INDUSTRIAS

---

Temos a satisfação de encaminhar nossa proposta técnica e comercial que tem por objetivo oferecer nossos produtos e serviços de tecnologia.

Nossa proposta foi desenvolvida de acordo com os requisitos a nós apresentados pelo estudo de caso e acreditamos que ela forneça as informações suficientes e necessárias para nossa seleção como parceiro. Entretanto, caso sejam necessários maiores detalhes, estamos à disposição para quaisquer esclarecimentos.

Reconhecemos a importância desse projeto para a sua organização e estamos comprometidos com o seu sucesso. Somos os responsáveis designados para servir de ponto de contato para a discussão de qualquer assunto relacionado com nossa proposta.

Agradecemos à atenção e enfatizamos o interesse em poder colaborar com a **PROTECH FABRICANTE DE COMPONENTES INDUSTRIAIS.**

Atenciosamente,

Daniel Henrique

[daniel.rodrigues41@fatec.sp.gov.br](mailto:daniel.rodrigues41@fatec.sp.gov.br)

RA 2830972313028

Luiz Felipe Rosa

[luiz.moura9@fatec.sp.gov.br](mailto:luiz.moura9@fatec.sp.gov.br)

RA 2830972313022

Maicon Wansley

[maicon.silva18@fatec.sp.gov.br](mailto:maicon.silva18@fatec.sp.gov.br)

RA 2830972313002

Vitor Almeida

[vitor.silva231@fatec.sp.gov.br](mailto:vitor.silva231@fatec.sp.gov.br)

RA 2830972313014

Yuri Gabriel

[yuri.silva39@fatec.sp.gov.br](mailto:yuri.silva39@fatec.sp.gov.br)

RA 2830972313021



## TERMO DE CONFIDENCIALIDADE

---

A **CONSUTECH CONSULTORIA DE TI** garante que utiliza padrões mundiais de ética profissional e confidencialidade. Portanto, não divulgará qualquer informação interna da CONTRATANTE que venha a conhecer durante a vigência da prestação de serviços. Sendo que, qualquer divulgação só será feita com o consentimento, por escrito, da mesma.

Por parte da CONTRATANTE, os dados desta proposta não devem ser revelados, duplicados ou usados, no todo ou em parte, para qualquer fim que não seja a avaliação

Os preços e as informações desta proposta que se referem a: arquitetura, programas, produtos e serviços, devem ser tratados como confidenciais e segredos comerciais da **CONSUTECH CONSULTORIA DE TI** e não devem ser usadas ou reveladas sem permissão, inclusive pelos profissionais da CONTRATANTE, seus gerentes, agentes ou contratados, diretamente relacionados ou não, com a avaliação desta proposta, aos quais, também se aplicam às restrições de uso deste documento.

Todos os esforços foram feitos para identificar as informações sobre marcas registradas. Entretanto, caso tais informações de propriedade tenham sido omitidas acidentalmente ao se fazer referência a certos produtos em particular, ou em qualquer outro caso, alerta e reitera a PROPONENTE que os nomes de produtos eventualmente não assinalados como vinculados ao direito de propriedade de terceiros podem ter marcas registradas de titularidade dos seus respectivos detentores.



## SUMÁRIO

---

<b>1. AVALIAÇÃO DO AMBIENTE .....</b>	6
<b>1.1 IDENTIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO CRÍTICOS .....</b>	6
<b>1.2 AVALIAÇÃO DAS AMEAÇAS E VULNERABILIDADES EXISTENTES .....</b>	6
<b>1.2.1 ADVERSARIAL .....</b>	6
<b>1.2.2 ACIDENTAL .....</b>	7
<b>1.2.3 ESTRUTURAL .....</b>	7
<b>1.2.4 AMBIENTAL .....</b>	7
<b>1.3 IDENTIFICAÇÃO DAS REGULAMENTAÇÕES E NORMAS APLICÁVEIS .....</b>	8
<b>1.3.1 LGPD .....</b>	8
<b>1.3.2 ITIL .....</b>	8
<b>1.3.3 COBIT .....</b>	8
<b>2. DESENVOLVIMENTO DO PLANO DE IMPLEMENTAÇÃO .....</b>	9
<b>2.1 ESTABELECIMENTO DO COMITÊ DE SEGURANÇA .....</b>	9
<b>2.2 DEFINIÇÃO DE ESCOPOS E LIMITES DO SGSI .....</b>	9
<b>2.3 ALOCAÇÃO DE RECURSOS HUMANOS E FINANCEIROS .....</b>	10
<b>3 ATENDIMENTO AOS REQUISITOS DA ISO 27001 .....</b>	11
<b>3.1 IMPLEMENTAÇÃO DOS CONTROLES DE SEGURANÇA .....</b>	11
<b>3.1.1 CONTROLES ADMINISTRATIVOS .....</b>	11
<b>3.1.2 CONTROLES TÉCNICOS .....</b>	12
<b>3.1.3 CONTROLES FÍSICOS .....</b>	12
<b>3.1.4 ANEXO A - PLANEJAMENTO FÍSICO RECOMENDADO .....</b>	13
<b>3.2 DESENVOLVIMENTO DE PROCEDIMENTOS OPERACIONAIS PADRÃO .....</b>	14
<b>3.3 TREINAMENTO DE FUNCIONÁRIOS EM SEGURANÇA DA INFORMAÇÃO .....</b>	14
<b>3.3.1 TREINAMENTO INTERNO .....</b>	14
<b>3.3.2 TREINAMENTO EXTERNO .....</b>	14
<b>3.4 REALIZAÇÃO DE AVALIAÇÃO DE RISCOS REGULARES .....</b>	15
<b>3.5 AVALIAR OS OBJETIVOS DE CONTROLE E CONTROLES .....</b>	16
<b>4 CUSTOS E TEMPO DE RESOLUÇÃO DE ATENDIMENTO .....</b>	17



# PLANO DE IMPLEMENTAÇÃO DE SGSI

---

## 1. AVALIAÇÃO DO AMBIENTE

O planejamento para implementação do SGSI conforme os padrões da ISO 27001 visa garantir a segurança de quaisquer ativos de informação críticos, garantir a confidencialidade, a integridade e a disponibilidade dos dados assim atendendo as regulamentações do setor. A base do planejamento serão quatro tópicos, sendo eles: a avaliação inicial da situação; o desenvolvimento do plano de Implementação; o atendimento aos requisitos da ISO 27001 e a apresentação do plano de implementação.

### 1.1 IDENTIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO CRÍTICOS

Os ativos identificados na operação da **TechPro** incluem projetos de engenharia (como especificações de produtos para clientes), dados de pesquisa e desenvolvimento, informações financeiras da instituição e de clientes; Informações de recursos humanos (como dados de colaboradores); Informações de perímetro; informações sobre processo fabril e métodos de produção/operação - como maquinários).

### 1.2 AVALIAÇÃO DAS AMEAÇAS E VULNERABILIDADES EXISTENTES

A avaliação foi realizada em cima do método de gerenciamento de ameaças cibernéticas encontradas no mercado. Esse tópico foi segregado em algumas categorias de risco, dessa forma facilitando averiguação do cenário geral:

#### 1.2.1 ADVERSARIAL

Foi identificado uma presença significativa de ameaças adversariais, como: ataques de phishing direcionados aos funcionários, ataques de ransomware visando os sistemas críticos da empresa e uma exposição contínua a ataques de negação de serviço (DDoS).



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 1.2.2 ACIDENTAL

Foi identificado sérios riscos relacionados a erros humanos, que levam a vazamentos de dados sensíveis, como a divulgação inadvertida de informações confidenciais por colaboradores. Além disso, existe uma tendência preocupante de instalação de software malicioso por descuido, o que aumenta o risco de comprometimento da segurança dos sistemas assim como o uso de dispositivos removíveis pessoais de armazenamento.

### 1.2.3 ESTRUTURAL

Foi levantado vulnerabilidades de softwares na infraestrutura, juntamente com configurações inadequadas de segurança que deixam os sistemas expostos a ameaças. Além disso, a falta de aplicação regular de patches de segurança aumenta o risco de ataques, pois a falta de atualização, deixa de corrigir erros e vulnerabilidades importantes nos sistemas.

### 1.2.4 AMBIENTAL

Reconhecemos a possibilidade de desastres naturais, como terremotos e incêndios, que representam uma ameaça física à infraestrutura de rede. Além disso, falhas de energia recorrentes têm o potencial de interromper as operações e causar indisponibilidade dos sistemas ainda mais considerando a falta de um gerador de energia nas instalações.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 1.3 IDENTIFICAÇÃO DAS REGULAMENTAÇÕES E NORMAS APLICÁVEIS

Após avaliação detalhada do cenário em que se encontra a organização, serão aplicados os procedimentos de segurança em cima das definições das leis e práticas a serem seguidas para garantir o escopo de segurança proposto a nível internacional, sendo as principais:

#### 1.3.1 LGPD

Promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

#### 1.3.2 ITIL

Modelo de referência para gerenciamento de processos de TI.

#### 1.3.3 COBIT

Guia de boas práticas apresentado como framework e mapas de auditoria, conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 2. DESENVOLVIMENTO DO PLANO DE IMPLEMENTAÇÃO

Para o desenvolvimento do plano de Implementação foram estabelecidos outras três etapas a serem explorados, sendo elas:

#### 2.1 ESTABELECIMENTO DO COMITÊ DE SEGURANÇA

Após análise da estrutura hierárquica da TechPro, ficou alinhado que o comitê de segurança da informação terá a seguinte composição:

I – Gestor de segurança da informação da CosuTech, que o coordenará.

II – O titular de tecnologia da informação da unidade.

III – O representante da Secretaria-Executiva da unidade.

IV – Os representantes de cada um dos setores críticos da unidade (pesquisa e desenvolvimento, financeiro, recursos humanos, supply chain, jurídico e operacional).

#### 2.2 DEFINIÇÃO DE ESCOPOS E LIMITES DO SGSI

A **ConsuTech** pretende se responsabilizar por todo o planejamento para a implementação do SGSI, ficará responsável por **implementar e manter** apenas a segurança lógica do cliente e o treinamento dos funcionários, já a parte física a **Consutech** se responsabiliza por desenhar o projeto e fornecer os insumos para a implementação inicial, **mas não por manter o funcionamento**, visto que a Protech possui sua equipe interna de infraestrutura de TI.

É de extrema importância a conformidade da segurança de rede física, caso a contratante não esteja dentro dos padrões mínimos recomendados do projeto, a Consutech atua podendo indicar parceiros, instituições e/ou empresas que possam se responsabilizar com certos aspectos da proposta e realizar a implantação física e configuração de segurança, assim como o perímetro da sala de T.I. A isenção da implementação da segurança física se dá pelo modelo de negócio da ConsuTech, que possui foco em consultoria e soluções lógicas.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 2.3 ALOCAÇÃO DE RECURSOS HUMANOS E FINANCEIROS

Para a implementação do Sistema de Gestão de Segurança da Informação (SGSI) na TechPro, estimamos um total de 500 horas de trabalho. Essa alocação inclui análise, planejamento, treinamento e execução das atividades relacionadas à segurança da informação.

**Dias:** Considerando uma jornada de trabalho de 8 horas por dia, o projeto levará aproximadamente 62 dias.

**Meses:** Considerando 20 dias por mês, o projeto será concluído em cerca de 3 meses.

Considerando o valor médio da hora de trabalho dos profissionais envolvidos, estabelecemos um custo de **R\$ 300,00 por hora**. Esse valor leva em conta as habilidades específicas necessárias para a implementação do SGSI e a experiência dos colaboradores.

#### **Os serviços oferecidos durante a implementação do SGSI incluem:**

**I - Análise de riscos e vulnerabilidades:** Identificação e avaliação das ameaças e vulnerabilidades específicas da TechPro; Priorização dos riscos com base na probabilidade e impacto.

**II - Desenvolvimento de Políticas e Procedimentos:** Elaboração de políticas de segurança da informação alinhadas aos requisitos da ISO 27001; Definição de procedimentos para lidar com incidentes de segurança.

**III - Treinamento e Conscientização:** Capacitação dos colaboradores sobre boas práticas de segurança; Sensibilização para a importância da proteção dos ativos de informação.

**IV - Implementação de Controles Técnicos:** Configuração de firewalls, antivírus e outras ferramentas de segurança; Monitoramento contínuo da rede e sistemas.

**V - Auditoria e Certificação:** Realização de auditorias internas para verificar a conformidade com os padrões da ISO 27001; Preparação para a certificação oficial.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 3 ATENDIMENTO AOS REQUISITOS DA ISO 27001

Visando o atendimento aos requisitos da ISO 27001 mais cinco etapas se provam necessárias, que consistem em:

#### 3.1 IMPLEMENTAÇÃO DOS CONTROLES DE SEGURANÇA

Visando atender as três etapas de gerenciamento (ações de prevenção, detecção e correção) e para melhor adequação da empresa as políticas de melhores práticas os controles de segurança foram divididos em três principais segmentos, sendo eles:

##### 3.1.1 CONTROLES ADMINISTRATIVOS

Consistem em procedimentos e políticas que uma empresa implementa ao lidar com informações confidenciais. Nessa categoria as seguintes medidas serão implementadas:

- I - Políticas e procedimentos de gerenciamento de ativos;
- II- Políticas de renovação e força da senha;
- III - Políticas e grupos de controle de acesso com base na função;
- IV - Políticas de renovação e força da senha;
- V - Treinamento de usuários;
- VI - Crachás de funcionários;
- VII - Contratação de equipe de segurança especial.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 3.1.2 CONTROLES TÉCNICOS

Envolvem hardwares e/ou softwares implementados para gerenciar riscos e oferecer proteção. Dentro deste contexto serão implementadas as seguintes medidas:

- I - Controle de acesso a edifícios com base em cartão;
- II - Proteção do sistema de dispositivos de rede;
- III - VPN para trabalho remoto;
- IV - Criptografia de dados dos registros de clientes;
- V - Backup de dados e do sistema operacional abrangente;
- VI - Firewalls de rede ou IPS;
- VII - Firewalls e antivírus baseados em host;
- VIII - Contenção e remoção de malware;
- IX - Monitoramento de segurança de rede;
- X - Restauração de dados e imagens de disco do backup;
- XI - Gerenciamento robusto de patches;
- XII - Monitoramento de segurança de rede;
- XIII - Restauração de dados e imagens de disco do backup;
- XIV - Gerenciamento robusto de patches.

### 3.1.3 CONTROLES FÍSICOS

São mecanismos como cercas e bloqueios implantados para proteger sistemas, instalações, pessoal e recursos. A ConsuTech elabora o projeto, porém, não se responsabiliza pela implementação de equipamentos para a conformidade dos controles físicos, podendo indicar quem a realize (vide ANEXO A). As seguintes medidas fazem parte dos controles físicos recomendados:

- I - Acesso exclusivo do administrador ao data center e instalações de rede;
- II - Avaliação de vulnerabilidade e teste de detecção;
- III - Detectores de fumaça;
- IV - Sistemas de sprinklers;
- V - Geradores de energia de backup para sistemas essenciais;
- VI - Monitoramento CFTV;
- VII - Manutenção regular de sistemas e equipamentos;
- VIII - Substituição rápida de equipamentos essenciais danificados ou com mau funcionamento;
- IX - Inventário de peças sobressalentes.

## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 3.1.4 ANEXO A - PLANEJAMENTO FÍSICO RECOMENDADO

**ITEM 0 – RACK PARA MONTAGEM SERVIDOR:** Dell APC Rack NetShelter SX 42U 19"  
600mm x 1070mm;

**ITEM 1 - CABEAMENTO CAT6:** 1 caixa com 300 metros, Furukawa;

**ITEM 2 – LINK 1 PRINCIPAL:** Internet dedicada com redundância de 1 Gbps;

**ITEM 3 – LINK 2 BACKUP:** Redundância de Internet Banda Larga de até 1 GBPs;

**ITEM 4 – FIREWALL FORTINET:** Proteção DDoS, IDS/IPS, balanceamento de carga de rede, regras de entrada e saída, restrições de acesso por localidade;

**ITEM 5 – SWITCH GERENCIÁVEL 48PT. GIGABIT:** Criação de VLAN por setor para otimização do tráfego de rede, gerenciamento e liberação de portas;

**ITEM 6 – SERVIDOR DE ARQUIVOS:** Computador com armazenamento de até 10TB, com RAID ativo – espelhamento de HD, redundância de fonte de energia – troca quente, criptografia dos dados e rotinas de backup automatizadas;

**ITEM 7 – SERVIDOR DE APLICAÇÃO + AUTENTICAÇÃO:** Maquina específica para comportar o sistema de SGSI

**ITEM 8 – 2 NOBREAKS DE 5000VA + MÓDULO EXTERNO COM 2 BATERIAS DF500:**  
Equipamento para suportar queda de energia da estrutura por até 5 horas;

**ITEM 9 – DVR SISTEMA DE CÂMERAS PARA VISIBILIDADE DA ESTRUTURA FÍSICA DA REDE:** Cameras externas posicionadas na entrada da sala + cameras internas da sala de T.I.

**ITEM 10 – CONTROLE DE ACESSO FACIAL OU POR CARTÃO PARA ENTRADA RESTRITA**

## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 3.2 DESENVOLVIMENTO DE PROCEDIMENTOS OPERACIONAIS PADRÃO (POP)

Tem como objetivo proteger ativos de informação críticos e cumprir com as regulamentações aplicáveis além de ser um instrumento de apoio à padronização dos processos, visando minimizar erros, desvios e variações em processos. Este POP aplica-se a todos os departamentos e colaboradores da TechPro envolvidos na gestão de ativos de informação críticos. Fica estabelecido que o comitê de segurança será responsável pela supervisão e implementação do SGSI, enquanto o departamento de TI fará a identificação de ativos de informação críticos e avaliação de ameaças e vulnerabilidades, o setor de recursos humanos por sua vez garantirá a conformidade com a LGPD e outras regulamentações aplicáveis.

### 3.3 TREINAMENTO DE FUNCIONÁRIOS EM SEGURANÇA DA INFORMAÇÃO

Para maior conscientização e conformidade com os procedimentos de segurança provou-se extremamente necessário o treinamento dos funcionários, de forma que o compartilhamento de conhecimento ocorra alinhado com as diretrizes da empresa para a adoção de estratégias futuras. Tendo isso em vista foram estabelecidos os seguintes treinamentos a serem realizados:

#### 3.3.1 TREINAMENTO INTERNO

Ocorre na empresa e é dividido em duas etapas, uma introdutória, fornecendo informações iniciais aos colaboradores quando eles entram na empresa, e outra de acompanhamento contínuo, para fortalecer e aplicar os conhecimentos ao longo do tempo.

#### 3.3.2 TREINAMENTO EXTERNO

Será realizado fora do local de trabalho, através de palestras, workshops e cursos para complemento dos conhecimentos adquiridos nos treinamentos internos. Esse tipo de aprendizado proporcionará aos colaboradores o treinamento de especialistas específicos de suas áreas.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

### 3.4 REALIZAÇÃO DE AVALIAÇÃO DE RISCOS REGULARES

Empresas usam análise de riscos para avaliar os impactos causados por incidentes e assim poder garantir a eficiência do gerenciamento de riscos, garantir que as ações implementadas atendam todos os objetivos.

A **ConsuTech** segue uma premissa que o processo de análise deve ser orientado por alguns fatores que são pontos chaves para um troubleshooting eficaz.

- I - Identificação de ativos e seus valores;
- II - Identificação de ameaças e vulnerabilidades;
- III - Qualificação de ameaças identificadas o impacto que ela causa e a probabilidade de ocorrência;
- IV - Impacto da ameaça x o custo operacional da contramedida.

Com esses pontos identificados seguimos para outros dois métodos que são pontos importantes no processo de avaliação de riscos a análise de risco quantitativa e a análise de risco qualitativa.

A **análise quantitativa** atribui números para o processo de análise tais como: Valor do ativo, custo de reposição do ativo, um ativo pode ter seu valor medido por receita adquirida pelo seu uso entre outros fatores. Nessa etapa do processo são levados em conta alguns pontos:

- I - Fator de exposição: É um valor subjetivo expresso como porcentagem, sendo contabilizado de 0,0 a 1,0 sendo 1,0 igual a 100%
- II - Taxa anual de ocorrência: É probabilidade de ocorrer uma perda durante o ano devido a um risco. Essa escala pode chegar a ser maior que 100% se um incidente ocorrer mais de 1 vez por ano.
- III - Expectativa de perda anual: Essa métrica da uma perspectiva de quanto se deve investir para proteção de ativos.



## PLANO DE IMPLEMENTAÇÃO DE SGSI

---

Na análise qualitativa utiliza-se de cenários que possam descrever a probabilidade e o impacto de uma ameaça. Nela utilizamos uma matriz de riscos para quais riscos a organização precisa priorizar e quais respostas desenvolver. Os resultados da matriz são usados como guia para a empresa executar alguma ação mediante aos riscos.

### 3.5 AVALIAR OS OBJETIVOS DE CONTROLE E CONTROLES

A avaliação de controle e controles tem como objetivo identificar os resultados alcançados e compará-los com os resultados almejados, esse método ajuda a identificar desvios de projetos e assim ser possível reavaliar e implementar mudanças para alcançar as metas desejadas.

O uso de indicadores de metas são peças fundamentais para que possamos chegar no resultado desejado através dos resultados dos indicadores, é possível comparar o resultado real com os objetivos, analisar os desvios e tomar uma ação corretiva com os resultados obtidos.

Esse processo é importante, pois através dele será possível fazer um acompanhamento das ações tomadas e avaliar a eficiência e gerar aprendizado organizacional para revisões no próprio planejamento.

Com isso o objetivo desta avaliação é garantir que o projeto inicial alcance as metas estabelecidas de forma que identifique falhas, para que ações sejam tomadas para corrigi-las e com isso gerar aprendizado para a organização e o projeto em revisões futuras.



## CUSTOS E ORÇAMENTO

---

### INVESTIMENTO

SERVIÇO PRESTADO		
CÓDIGO	DESCRÍÇÃO	V. TOTAL (R\$)
10101	500x Horas de projeto para implementação do plano.	R\$ 150.000

Tempo estimado: 3 meses (8h diárias - Segunda à Sexta)

Valor hora: R\$ 300,00

### OPCIONAL - SERVIÇO DE SUPORTE MENSAL APÓS IMPLEMENTAÇÃO

(OPCIONAL) - SUPORTE MENSAL		
CÓDIGO	DESCRÍÇÃO	V. TOTAL (R\$)
10101	10x Horas de suporte mensal.	R\$ 2.500

### TEMPO DE RESOLUÇÃO PARA ATENDIMENTO

ACORDO DE NÍVEL DE SERVIÇO (ANS)		
Processo	Cobertura	Nível de Serviço
Atendimento à incidentes e requisições	08 horas por dia – 5 dias por semana (segunda à sexta-feira – 09h00 às 18h00)	SLA de 95% dentro do prazo
Atendimento Plantão	de segunda à sexta-feira das 18:01 às 08:59 e finais de semana	SLA de 90% dentro do prazo

TEMPOS DE ATENDIMENTO		
Nível	Detalhamento	Resposta
<b>Critico</b>	Indisponibilidade Generalizada	Em até 30 minutos
<b>Alto</b>	Lentidão e correção de erros	Em até 02 horas
<b>Médio</b>	Inclusão, remoção e alteração de itens de configuração	Em até 04 horas
<b>Baixo</b>	Esclarecimentos de dúvidas em relação a recursos e funcionamento do sistema	Em até 08 horas



# ACEITE DE PROPOSTA

**Desenvolvendo o futuro tecnológico da sua empresa com foco no crescimento**

O pedido de compra deve conter todas as informações necessárias para faturamento, entrega e cobrança, além da documentação de cadastro eventualmente se for requisitada.

O aceite deverá ser formalizado por um contrato após com um “de acordo” nesta proposta por pessoa autorizada para tal ato na empresa compradora, firmando compromisso.

**APROVAMOS TODOS OS TERMOS E CONDIÇÕES DA PROPOSTA:**

NOME:	ASSINATURA:
DATA:	CNPJ:



## ENTRE EM CONTATO

FICAREMOS HONRADOS EM ATENDÊ-LO

**+55 11 94826-5894 | +55 11 98560-4057**

**[contato@consutech.com.br](mailto:contato@consutech.com.br)**

Av. Ten. Marques, 5136 - Chácara do Solar I (Fazendinha), Santana de Parnaíba - SP, 06530-001

2024



**IMPLEMENTAÇÃO DE SGSI**  
PROTECH - FABRICANTE DE COMPONENTES INDUSTRIAIS

Daniel Henrique dos Santos Rodrigues  
Luiz Felipe Rosa Moura  
Maicon Wansley Antunes da Silva  
Vitor Almeida da Silva  
Yuri Gabriel Jales da Silva