**PROPOSTA TÉCNICA**

Stellantis Financiamentos

# Plano de Trabalho para Serviço Cybersecurity

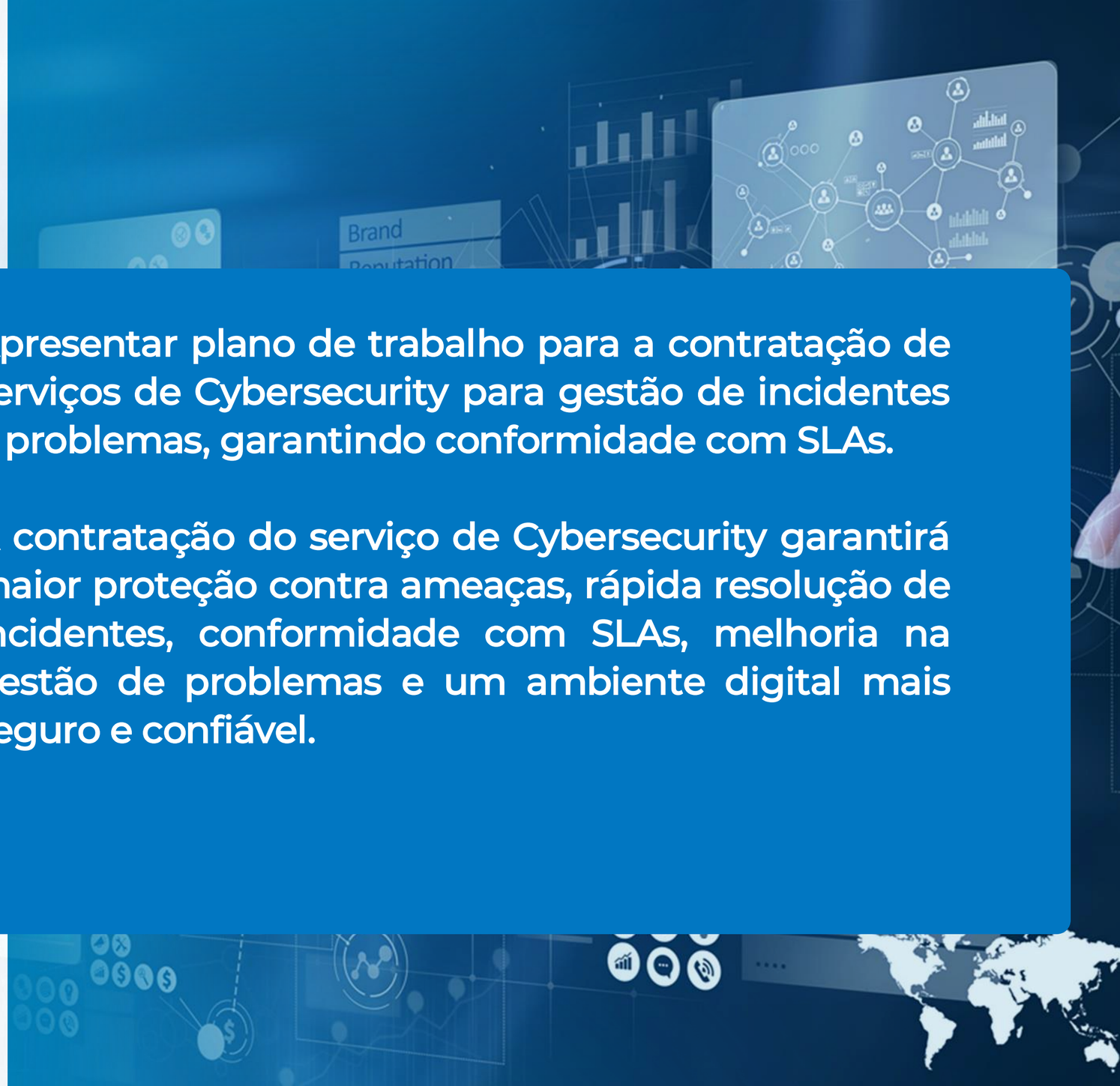
ID da Proposta PSA013-25 | Versão 1.0 | Data da Proposta 31/01/2025 | Validade 15 dias

MODALGR | STELLANTIS FINANCIAMENTOS

# OBJETIVO DESTA PROPOSTA

- Apresentar plano de trabalho para a contratação de serviços de Cybersecurity para gestão de incidentes e problemas, garantindo conformidade com SLAs.

- A contratação do serviço de Cybersecurity garantirá maior proteção contra ameaças, rápida resolução de incidentes, conformidade com SLAs, melhoria na gestão de problemas e um ambiente digital mais seguro e confiável.



# PLANO DE TRABALHO SERVIÇO CYBERSECURITY

MODALGR | STELLANTIS FINANCIAMENTOS

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

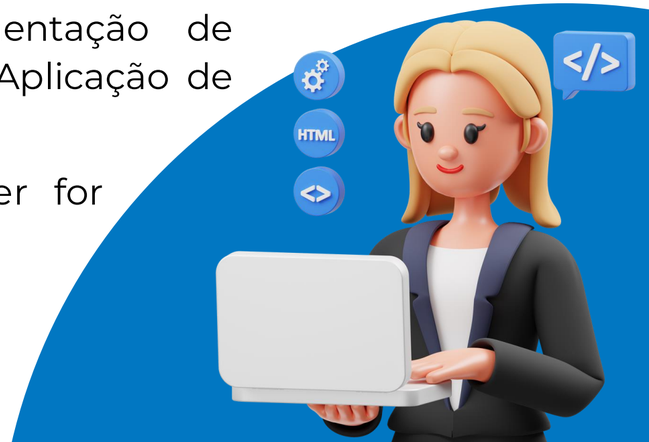
## 1 - Ações Críticas (Implementação Imediata - Primeiro Mês)

### 1.1 Proteção Contra Ransomware e Malware (Malware, Ransomware)

- **Política de Backup e Recuperação** → Implementação de backups em **múltiplos locais** (on-premise e cloud), utilizando **snapshotting e versionamento** para evitar que sejam corrompidos por ransomware. Testes regulares de recuperação garantem a integridade dos backups.
  - **Ferramentas:** Veeam, Acronis, AWS Backup, Azure Backup, Google Backup and DR.

- **EDR e Antivírus Avançado →** Soluções como **Endpoint Detection and Response (EDR)** detectam comportamentos suspeitos e interrompem ataques antes que causem danos.
  - **Ferramentas:** Qualys, CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, AWS GuardDuty, Google Security Command Center.

- **Segmentação de Rede e Privilégios Mínimos (Zero Trust)** → Implementação de **microsegmentação** para restringir acessos e minimizar impactos de invasões. Aplicação de **Least Privilege Access** para evitar movimentação lateral de malware.
  - **Ferramentas:** Qualys, CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, AWS GuardDuty, Google Security Command Center.



# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

## 1.2 Mitigação de Phishing e Engenharia Social (Phishing, Engenharia Social)

- **Autenticação Multifator (MFA) Obrigatória** → Implementação de MFA em **todos os acessos críticos** para impedir logins indevidos, mesmo que senhas sejam comprometidas.
  - **Ferramentas:** AKAMAI, Microsoft Entra ID MFA, AWS IAM MFA, Google Authenticator.

- **Treinamentos Urgentes para Colaboradores** → Realização de campanhas educacionais sobre phishing, com simulações reais de ataques.
  - **Ferramentas:** KnowBe4, Cofense, Microsoft Attack Simulation Training, AWS Security Awareness Training, Google Security Awareness Training, Microsoft Teams, Google Meet, Zoom.

- **Filtros Avançados de E-mail** → Implementação de filtros de e-mail com detecção de links e anexos suspeitos para evitar ataques de phishing.
  - **Ferramentas:** AKAMAI, AXUR, Proofpoint, Mimecast, Barracuda Email Security, Microsoft Defender for Office 365, AWS SES Email Protection, Google Workspace Security.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

## 1.3 Monitoramento e Resposta a Incidentes (Todos os Itens)

- **SIEM e SOAR para Detecção e Resposta Rápida** → Implementação de **Security Information and Event Management (SIEM)** para coleta e análise de logs de segurança, integrado com **Security Orchestration, Automation and Response (SOAR)** para resposta automatizada a incidentes.
  - **Ferramentas:** Splunk, Microsoft Sentinel, AWS Security Hub, Google Chronicle SIEM.

- **Plano de Resposta a Incidentes (IRP) Atualizado** → Revisão e teste de **playbooks de resposta** para cada tipo de incidente, garantindo uma reação rápida e eficiente.
  - **Ferramentas:** KnowBe4, Cofense, Microsoft Attack Simulation Training, AWS Security Awareness Training, Google Security Awareness Training, Microsoft Teams, Google Meet, Zoom.

## 2 - Ações de Alta Prioridade (Implementação em até 3 Meses)

### 2.1 Proteção Contra Ataques DDoS (DDoS)

- **Implementação de Soluções Anti-DDoS** → Utilização de serviços de mitigação que absorvem e filtram ataques volumétricos antes de atingirem a infraestrutura.
  - **Ferramentas:** Azure Load Balancer, AWS Elastic Load Balancer, Google Cloud Load Balancing.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

## 2 - Ações de Alta Prioridade (Implementação em até 3 Meses)

### 2.1 Proteção Contra Ataques DDoS (DDoS)

- **Implementação de Soluções Anti-DDoS** → Utilização de serviços de mitigação que absorvem e filtram ataques volumétricos antes de atingirem a infraestrutura.
    - **Ferramentas:** Azure Load Balancer, AWS Elastic Load Balancer, Google Cloud Load Balancing.

### 2.2 Gestão de Vulnerabilidades e Exploração de Falhas (Exploração de Vulnerabilidades, Man-in-the-Middle)

- **Pentests Regulares e Correção de Vulnerabilidades** → Condução de testes manuais e automatizados para identificar brechas antes que sejam exploradas.
    - **Ferramentas:** Qualys, Nessus, OpenVAS, OWASP ZAP, Burp Suite, NMAP, WireShark, Microsoft Defender Vulnerability Management, AWS Inspector, Google Security Command Center.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

- **Web Application Firewall (WAF) e Hardening de Aplicações** → Configuração de regras de WAF para bloquear tráfego malicioso e aplicação de **hardening** para remover configurações inseguras.
    - **Ferramentas:** AKAMAI, AWS WAF, Azure WAF, Google Cloud Armor.

## 2.3 Segurança de Dados e Prevenção de Vazamentos (Violações de Dados, Fraudes)

- **Criptografia de Dados em Trânsito e Repouso** → Aplicação de **TLS 1.2**+ para comunicações e **AES-256** para armazenamento.
    - **Ferramentas:** AKAMAI, HashiCorp Vault, AWS KMS, Azure Key Vault, Google Cloud KMS.
- **Gerenciamento de Identidade e Acessos (IAM) Reforçado** → Implementação de controles granulares para garantir que apenas usuários autorizados tenham acesso a dados sensíveis.
    - **Ferramentas:** AKAMAI, Okta, CyberArk, Microsoft Entra ID, AWS IAM, Google IAM.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

- **Monitoramento de Vazamento de Dados na Dark Web** → Uso de plataformas que analisam a dark web para detectar credenciais ou dados comprometidos.
    - **Ferramentas:** Axur, Recorded Future, SpyCloud, Microsoft Defender Threat Intelligence

## 3 - Ações Estratégicas e Contínuas (6 Meses ou Mais)

### 3.1 Treinamentos e Simulações Periódicas (Phishing, Engenharia Social, Ameaças Internas, Fraudes)

- **Simulações de Ataques de Engenharia Social e Phishing** → Execução contínua de campanhas para reforçar o comportamento seguro dos funcionários.
    - **Ferramentas:** Outlook, Gmail, Microsoft Attack Simulation Training, AWS Security Awareness Training, Google Phishing Protection.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

### 3.2 Auditorias, Conformidade e Resiliência Cibernética (Violações de Dados, Fraudes, Todos os Itens)

- **Auditorias de Segurança e Revisão de Controles** → Revisão de configurações, logs e acessos para garantir conformidade com normativas como **LGPD**, **GDPR**, **ISO 27001**.
  - **Ferramentas:** Microsoft Purview Compliance Manager, AWS Audit Manager, Google Assured Workloads.

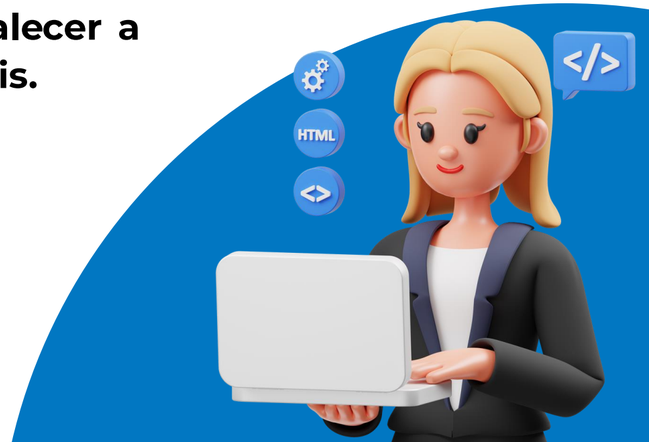
- **Testes de Continuidade de Negócios (BCP) e Recuperação de Desastres (DRP)** → Simulações para validar os tempos de recuperação de serviços e dados após um incidente.
  - **Ferramentas:** Azure Site Recovery, AWS Elastic Disaster Recovery, Google Backup and DR.

# QUAL SERÁ NOSSO PLANO DE TRABALHO ?

## Cronograma de ações

| Entregáveis | Mês 1 | Mês 2 | Mês 3 | Mês 4 | Mês 5 | Mês 6 | Mês 7 | Mês 8 |
|---|---|---|---|---|---|---|---|---|
| **Kick off e liberação de acessos** | Kickoff e liberação de acessos | | | | | | | |
| **Ações Críticas (Implementação Imediata - Primeiro Mês)** | Ações Críticas (Implementação Imediata - Primeiro Mês) | | | | | | | |
| **Ações de Alta Prioridade (Implementação em até 3 Meses)** | | Ações de Alta Prioridade (Implementação em até 3 Meses) | | | | | | |
| **Ações Estratégicas e Contínuas (6 Meses ou Mais)** | | | Ações Estratégicas e Contínuas (6 Meses ou Mais) | | | | | |

- **Essas ações têm como objetivo a implementação de políticas e ferramentas para fortalecer a segurança cibernética, garantindo a mitigação de ameaças e a proteção dos ativos digitais.**



# ESCOPO DE SERVIÇOS - Suporte

## Procedimentos para Atendimento

1. **Recebimento de Incidente ou Solicitação:** O incidente ou solicitação será registrado no sistema de gerenciamento de serviços.

2. **Classificação e Priorização:** A equipe de suporte irá classificar e atribuir a severidade e prioridade conforme a descrição do incidente.

3. **Resposta Inicial:** A equipe de suporte realizará a primeira resposta dentro do tempo especificado no SLA.

4. **Resolução:** A resolução será dada conforme o tempo de resposta e resolução definido no SLA, com comunicação contínua ao cliente sobre o status.

5. **Fechamento:** Após a resolução, o incidente será fechado, sendo registrado no sistema e, se necessário, realizadas ações de melhoria para evitar recorrências.

# Impulsione seu negócio com **tecnologia de resultado!**

**Escaneie** para falar com o nosso time

MODALGR®

+55 (13) 4101.0010

comercial@modalgr.io

**MATRIZ BRASIL**

R. Visc. de Rio Branco,
02 - 6º Andar
Centro, Santos - SP

**PORTUGAL**

Rua Fernanda Seno, 6
7005-485 / Évora

MODALGR®

# *Thinking Innovation*

Transformando negócios através da **tecnologia** e **inovação**.