ETP – Estudo Técnico Preliminar

AV – Análise de Viabilidade

1 IDENTIFICAÇÃO DO PROJETO

Identificação do Projeto			
Projeto:	Contratação de serviços gerenciados de segurança cibernética		
Gerente de Projeto:	Fernando Felipe Andrade		
Líder Técnico:	Márcio Henrique C. d'Ávila		
Unidade organizacional:	DIRFOR	**Gerência:**	ATEND

2 PROCESSO DE CONTRATAÇÃO

Processo SEI nº 0813428-76.2023.8.13.0000.

3 FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1 Contextualização, necessidade e motivação da contratação

A segurança da informação vem evoluindo e crescendo continuamente nas últimas décadas e, no mundo digital e interconectado, se denomina cibersegurança ou segurança cibernética, caracterizada pelo gerenciamento de riscos de segurança da informação e a salvaguarda de pessoas, organizações e sociedades contra vulnerabilidades, ameaças e ataques, quando a informação está em forma digital em computadores, armazenamento e redes. Engloba também temas como continuidade de negócios e resiliência organizacional, tratamento e resposta a incidentes de segurança, forense digital.

O universo de cibersegurança é muito amplo e complexo. Exige conhecimentos altamente especializados, atualização constante, atuação dinâmica e eficaz, em suma, grandes e variados esforços, organização, orquestração e governança em termos de processos, pessoas e ferramentas. Organizações de referência internacional, governamentais e independentes da comunidade, tem difundido e atualizado constantemente inúmeros padrões, modelos (frameworks) e melhores práticas de cibersegurança: International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) dos Estados Unidos, Center for Internet Security (CIS), MITRE (originário do Massachussets Institute of Technology), a fundação de código aberto Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), dentre outras.

Fatores recentes ampliaram e aceleraram muito os desafios e necessidades, de forma urgente e sem precedentes:

- O uso ainda mais crítico, intensivo, complexo e distribuído de tecnologia da informação, serviços e recursos digitais nas atividades fim e administrativas, dentro e fora das dependências do Tribunal, com os adventos da pandemia de COVID-19, do teletrabalho e da crescente adoção de serviços em nuvem.

- As demandas decorrentes da entrada em vigor da Lei Federal nº 13.709 de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- As exigências decorrentes da Resolução CNJ nº 396 de 07/06/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Casos recentes cada vez mais frequentes de ameaças avançadas e direcionadas, incidentes em instituições públicas e privadas próximas, de ataques como ransomware (sequestro digital), fraudes, vazamento de dados, hacktivismo (ativismo político hacker).

Há grande dificuldade atual em formar e contratar pessoal qualificado em segurança cibernética, pois a demanda está muito aquecida[1]. A pesquisa anual (ISC)² Cybersecurity Workforce Study 2022[2], que entrevistou 11.779 especialistas e tomadores de decisão no mundo, mostra que embora a força de trabalho global em cibersegurança tenha crescido 11,1% no ano (+18,3% no Brasil), a demanda por estes profissionais cresceu mais ainda, com o déficit (gap) crescendo globalmente 26,2% em relação ao ano anterior. No Brasil, o gap em 2022 recuou, mesmo assim a pesquisa estima um déficit de quase 313 mil profissionais em cibersegurança para atender a demanda no país. Mesmo empresas especializadas têm dificuldade em recrutar e manter pessoal qualificado, com grande rotatividade (*turnover*) e elevação de salários[3]. A mesma pesquisa aponta que 21% dos respondentes da América do Norte mudaram de emprego nos últimos 12 meses, contra 13% no ano anterior.

No **TRIBUNAL**, acrescente-se ainda a dificuldade em viabilizar, do ponto de vista normativo e operacional, o uso de servidores públicos do órgão em regime de escalas de trabalho 24×7 para os serviços que são de natureza contínua e ininterrupta.

As tecnologias em cibersegurança tem avançado contínua e aceleradamente, incluindo aplicação intensiva de inteligência artificial, aprendizado de máquina e automação, visando aumentar a eficiência e eficácia na detecção e resposta a ameaças e ataques, bem como por vezes compensando parte da necessidade de atuação humana.

Para evoluir seus recursos e fazer frente às atuais obrigações e ameaças cibernéticas, a DIRFOR precisa realizar maciço investimento na tríade de pessoas, processos e tecnologias em governança, gestão e operações de segurança cibernética do **TRIBUNAL**. E o caminho natural para a DIRFOR cumprir tal necessidade de forma ágil e adequada é recorrer ao mercado especializado, onde já estão provedores de serviços capazes de prover e operacionalizar o estado da arte em tecnologias e processos para cibersegurança, atuando com equipe de profissionais especializados e experientes.

3.2 Objetivos a serem alcançados com a contratação

A solução deve prover serviços gerenciados de segurança cibernética em três pilares:

- Governança e gestão de segurança cibernética de forma centralizada no âmbito de tecnologia da informação e comunicação (TIC), por meio de serviços estratégicos de governança, risco e conformidade (GRC) e definições de controles, salvaguardas e remediações;

[1] LinkedIn Pulse. Demanda global por profissionais de cibersegurança é urgente!, por Camila Farani, 25/10/2022, disponível em https://www.linkedin.com/pulse/demanda-global-por-profissionais-de-ciberseguran%C3%A7a-%C3%A9-urgente-farani/ .
[2] (ISC)². (ISC)² Cybersecurity Workforce Study, disponível em https://www.isc2.org/Research/Workforce-Study .
[3] Canaltech. Ataques elevam demanda e salários dos profissionais de cibersegurança no Brasil, por Márcio Padrão, 21/03/2022, disponível em https://canaltech.com.br/mercado/ataques-elevam-demanda-e-salarios-dos-profissionais-de-ciberseguranca-no-brasil-212062/ .

- Segurança defensiva (“blue team”) por meio de monitoramento, detecção e resposta gerenciados de segurança cibernética;
- Segurança ofensiva (“red team”) por meio da gestão contínua de exposição a ameaças e vulnerabilidades, incluindo testes de segurança.

Além disso, aspectos urgentes e correlatos de gestão de identidade e acesso devem também ser avaliados, visando tanto entender e integrar adequadamente o cenário atual destes aspectos nos serviços abrangidos, quanto nortear as iniciativas futuras do Tribunal:

- Levantamento e diagnóstico inicial de governança e gestão de identidades (IGA), gestão de acessos e autorizações (AM) e gestão de acessos privilegiados (PAM).

3.3 Benefícios resultantes da contratação

- Realizar ágil e maciço investimento na tríade de pessoas, processos e tecnologias em governança, gestão e operações de segurança cibernética do Tribunal, com aporte de pessoal técnico especializado, transferência de conhecimento, metodologia, padronização, estrutura operacional, ferramentas e soluções tecnológicas adequadas;
- Prover meios adequados e especializados, em termos de pessoas, processos e tecnologias, para a gestão, implementação e manutenção eficaz dos controles e salvaguardas de segurança cibernética e prover o apoio à gestão e à governança da segurança da informação, à continuidade de negócios em TIC e à gestão de riscos na Diretoria de Informática;
- Implantar um centro de controle e operações de segurança cibernética que componha as funções básicas de segurança de identificar, proteger, detectar, responder e recuperar, atuando tanto na segurança defensiva e reativa para monitoramento, detecção e resposta gerenciados a eventos e incidentes de segurança, quanto na segurança ofensiva e proativa para gestão contínua de vulnerabilidades e ameaças e para testes de segurança, prestando apoio direto às diversas áreas da DIRFOR na prevenção, investigação, remediação e melhorias de cibersegurança;
- Elevar o nível de segurança cibernética no Tribunal, sua maturidade e melhoria contínua, visando estabelecer o nível adequado de controle sobre a confidencialidade, integridade e disponibilidade dos ativos e serviços de TIC e das informações digitais do Tribunal;
- Garantir conformidade e alinhamento com os requisitos de negócio, regulamentos pertinentes, a tolerância a riscos e os recursos da organização, em especial observância à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Obter visibilidade ampla sobre a segurança cibernética, a superfície de ataque e os níveis de risco no Tribunal, tanto ao nível tático-operacional quanto ao nível estratégico-gerencial;
- Contribuir na comunicação, difusão e disseminação da cultura e sensibilização dos conceitos, práticas e controles de segurança cibernética na DIRFOR e em todo o Tribunal.

4 DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

4.1 Identificação das necessidades de negócio

4.1.1 Requisitos de negócio

Necessidade 1: Promover a Governança e gestão de segurança de TIC.

Requisito 1.1: Serviços estratégicos de governança, risco e conformidade (GRC)

- Diagnósticos e avaliações, com análises de gap (situação e lacunas), maturidade, progresso e melhoria contínua, contemplando, conformidade (leis, normas, melhores práticas, políticas, processos, planos e procedimentos), controles e atividades, papéis e responsabilidades, com periodicidade mínima anual;
    - Referências[4, 5]:
        - Nível global (arcabouço de governança): NIST Cybersecurity Framework (CSF) incluindo seus quatro Níveis (*Tiers*) de Implementação da Estrutura, normas ABNT NBR ISO/IEC 27001:2022 – Requisitos de Sistemas de gestão da segurança da informação, ABNT NBR ISO/IEC 27032:2015 – Diretrizes para segurança cibernética, ABNT NBR ISO/IEC 27004:2017 – Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação, Resolução CNJ nº 396/2021 – Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e seus Anexos na Portaria CNJ nº 162/2021;
        - Nível conceitual de controles: norma ABNT NBR ISO/IEC 27002:2022 – Controles de segurança da informação;
        - Nível de controles de segurança nas camadas lógica e física: CIS Critical Security Controls v8, considerando Perfil IG3 (ver seus mapeamentos[6] com ISO/IEC 27002:2022 e NIST CSF), NIST Special Publication (SP) 800-53 - Security and Privacy Controls for Information Systems and Organizations;
        - Common Criteria for Information Technology Security Evaluation (CC:2022 ou série ISO/IEC 15408:2022) e Common Methodology for Information Technology Security Evaluation (CEM:2022 ou ISO/IEC 18045:2022).
- Proposição, elaboração, análise, revisão e melhoria contínua das políticas, processos, planos e procedimentos de segurança da informação, segurança cibernética e proteção de dados do Tribunal, com base nas necessidades, na legislação e nos normativos vigentes aplicáveis (CNJ, Federal e Estadual), normas nacionais e internacionais e melhores práticas de mercado, visando orientar e sustentar, em termos normativos e regulatórios, a efetividade e eficácia das operações e práticas de segurança cibernética e consolidar um sistema de gestão de segurança da informação (SGSI);
    - Referências:
        - CNJ. Resolução nº 396 de 07/06/2021 - Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
        - CNJ. Portaria nº 162 de 10/06/2021 - Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;
        - TJMG. Portaria nº 4718/PR/2020 – Institui a Política de Segurança da Informação no âmbito da Tecnologia da Informação e Comunicação do TJMG e dispõe sobre o Modelo de Gestão de Segurança da Informação.
        - Gartner. Toolkit: Security Policy Exception, 03/03/2017, revisado em 09/11/2022, ID F00318663, por Sam Olvaei, Jeffrey Wheatman e Rob McMilan. Propõe um modelo para tratamento controlado e aprovação de exceções à política de segurança.
- Elaboração, implantação, testes e melhoria contínua de um plano de continuidade de negócios com foco no Processo Judicial Eletrônico (PJe) e sistemas complementares (como GuiasWeb e RUPE - Repositório Unificado de Procedimentos Eletrônicos), contemplando: elaboração completa de Análise de Impacto de Negócio (*business impact analysis* – BIA) incluindo entrevistas aos principais setores envolvidos na área judiciária, identificação dos processos de trabalho e/ou atividades envolvidas, avaliação dos impactos de disrupção, identificação e estabelecimento de período máximo tolerável de disrupção (*maximum tolerable period of disruption* – MTPD ou

[4] Gartner. Security Frameworks: The What and Why, and How to Select Yours, 04/02/2020, ID G00441470, por Mike Wonham, Joerg Fritsch, Michael Kranawetter.

[5] Gartner. Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes, 04/10/2019, revisado em 08/08/2022, ID G00380672, por Richard Addiscott, Jeffrey Wheatman, Khushbu Pratap.

[6] CIS. CIS Critical Security Controls Version 8 Mappings, https://www.cisecurity.org/controls/v8#v8-mappings , acessado em nov/2022.

maximum acceptable outage – MAO), ponto de recuperação objetivado (*recovery point objective* – RPO) e tempo de recuperação objetivado (*recovery time objective* – RTO); identificação, mapeamento e correlação dos ativos, recursos dependências e atividades de apoio que suportam o serviço de negócio; elaboração de plano de administração de crise (PAC), plano de continuidade operacional (PCO) e plano de recuperação de desastres (PRD); planejamento, elaboração e execução de testes, exercícios e revisão com periodicidade mínima anual, visando estabelecer e consolidar um sistema de gestão de continuidade de negócios (SGCN) com foco em TIC;

- Referências:
  - CNJ. Portaria nº 162 de 10/06/2021 – Anexo II – Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário;
  - ABNT NBR ISO 22301:2020 – Sistema de gestão de continuidade de negócios — Requisitos;
  - ABNT NBR ISO 22313:2020 – Orientações para o uso da ABNT NBR ISO 22301;
  - ISO/TS 22332:2021 – Guidelines for developing business continuity plans and procedures;
  - ISO 22398:2013 – Societal security — Guidelines for exercises.

- Elaboração, implantação, execução e melhoria contínua de um plano[7, 8] e processo de tratamento e resposta a incidentes de segurança cibernética, incluindo um plano específico para o gerenciamento de crises cibernéticas, visando maximizar a eficácia e minimizar os tempos de detecção e de resposta aos incidentes de segurança cibernética;
  - Referências:
    - CNJ. Portaria nº 162 de 10/06/2021, em especial os protocolos de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ); Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ);
    - ABNT NBR ISO 22320:2020 Diretrizes para gestão de incidentes;
    - ISO/IEC 27035-1:2023 Information security incident management — Part 1: Principles of incident management;
    - ISO/IEC 27035-2:2023 Information security incident management — Part 2: Guidelines to plan and prepare for incident response;
    - ABNT NBR ISO/IEC 27035-3:2021 Gestão de incidentes de segurança da informação Parte 3: Diretrizes para operações de resposta a incidentes de TIC;
    - ABNT NBR ISO/IEC 27037:2013 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
    - NIST SP 800-61 – Computer Security Incident Handling Guide Rev. 2;
    - FIRST.Org Computer Security Incident Response Team (CSIRT) Services Framework, versão 2.1.0, em especial as áreas de serviço "Information Security Event Management" e "Information Security Incident Management";
    - CREST Cyber Security Incident Response Guide, Version 1;
    - GSI/PR. Portaria nº 120 de 21/12/2022, Plano de Gestão de Incidentes Cibernéticos para a administração pública federal (PlanGIC), referencial de boa prática;
    - CIS Controle 17 - Gestão de respostas a incidentes.

- Estabelecimento, apuração, documentação e melhoria contínua de métricas, indicadores chave de desempenho (KPI), painéis (dashboards) técnico-operacional (foco em tecnologia) e estratégico-gerencial (foco no negócio) e lições aprendidas, com relatórios mensais de situação e desempenho;
  - Referência:
    - Gartner Cybersecurity Business Value Benchmark[9]: 16 métricas de níveis de proteção orientados a resultados.
- Revisão e melhoria contínua, de periodicidade máxima semestral, para todas as políticas, processos, planos, métricas e indicadores.
- Planejamento, elaboração, participação na execução e acompanhamento de planos de ação e campanhas para divulgação, conscientização, testes e implementação de normativos, processos e controles de segurança cibernética, incluindo a posterior avaliação da sua eficácia.

[7] Gartner. How to Create an Incident Response Plan, 06/03/2021, revisado em 10/11/2022, ID G00735337, por Eric Ahlm.
[8] Gartner. Toolkit: Cybersecurity Incident Response Plan, 08/12/2021, ID G00743169, por Wam Voster, William Candrick.
[9] Gartner. The Gartner Cybersecurity Business Value Benchmark, First Generation, 05/09/2022 - ID G00775537, por Paul Proctor, Srinath Sampath, Paul Furtado, Patrick Long, Lisa Neubauer, Deepti Gopal.

Requisito 1.2: Definição de controles, salvaguardas e remediações

- Análise, elaboração, documentação, acompanhamento e avaliação de um plano de ação plurimensal de controles e salvaguardas de segurança cibernética, medidas de remediação e mitigação, planejando ações para aplicação de atualizações de segurança, regras, barreiras e hardening de ativos de TIC, a partir dos resultados dos diagnósticos, análises, testes, eventos e incidentes de segurança, tanto proativos/preventivos (gestão de vulnerabilidades e melhores práticas internacionais) quanto reativos (tratamento de ameaças e incidentes).
    - Referências:
        - Normas internacionais ABNT NBR ISO/IEC 27002:2022, ABNT NBR ISO/IEC 29151:2020;
        - CIS Critical Controls v8 do Center for Internet Security (CIS);
        - NIST Special Publication (SP) 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations;
        - Cloud Controls Matrix (CCM) da Cloud Security Alliance (CSA).
- Priorização baseada em gerenciamento de riscos;
- Execução e acompanhamento contínuos do plano de ação, com relatórios quinzenais de progresso e situação.
    - Na maioria dos controles, onde os respectivos ativos já são suportados por serviços ou contratos específicos de sustentação, deve ser feito o repasse detalhado das ações a serem executadas, o acompanhamento do andamento, e prestado todo esclarecimento de dúvidas e apoio técnico consultivo necessário.
    - Para as ferramentas e soluções fornecidas pela contratada, deve incluir a efetiva aplicação dos controles.

Necessidade 2: Permitir, de forma unificada e contínua, o monitoramento, detecção e resposta gerenciados de cibersegurança.

Requisito 2.1: Centro de operações de segurança (SOC) e equipe de tratamento e resposta (ETIR)

- Utilizar um centro de operações de segurança (*security operations center* – SOC)[10, 11, 12, 13, 14] para monitoramento, detecção, investigação e resposta gerenciados (*managed detection and response* – MDR)[15] de eventos de segurança cibernética em regime 24x7, sendo que a contratada deve possuir ao menos dois SOCs com redundância;
- Estabelecer a equipe de tratamento e resposta a incidentes de segurança (ETIR), com atuação remota e local, incluindo Nível 1 (atuação inicial), Nível 2 (atuação avançada e em crises) e Nível 3 (especialistas);
    - Referência:
        - IETF. RFC 2350 - Expectations for Computer Security Incident Response, junho 1998, Best Current Practice (BCP 21).
- Definição, análise, atualização, melhoria e expansão dos casos de uso[16, 17] de monitoramento e detecção, bem como dos *playbooks* de tratamento, resposta e automação;

[10] Gartner. The Journey to SOC in Three Steps: Step 1 Planning and Prioritizing Objectives, 08/12/2022, ID G00777225, por Eric Ahlm, Steve Santos.
[11] Gartner. The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, 19/12/2022, ID G00777227, por Eric Ahlm.
[12] Gartner. The Journey to SOC in Three Steps: Step 3 Building Reporting and Maturity Roadmaps, 16/01/2023, ID G00777228, por Eric Ahlm.
[13] Gartner. How to Build and Operate a Modern Security Operations Center, 07/06/2021, ID G00743904, por Eric Ahlm.
[14] Gartner. SOC Model Guide, 19/10/2021, ID G00754096, por John Collins, Mitchell Schneider, Pete Shoard.
[15] Gartner. Market Guide for Managed Detection and Response Services, 14/02/2023, ID G00761083, por Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies.
[16] Gartner. How to Create and Maintain Security Monitoring Use Cases for Your SIEM, 12/07/2022, ID G00767954, por Eric Ahlm.

- Realizar os procedimentos cabíveis de análise e investigação forense pós-incidentes;
    - Referências:
        - CNJ. Portaria nº 162 de 10/06/2021, protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ);
        - ABNT NBR ISO/IEC 27037:2013 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
        - MITRE Open Vulnerability and Assessment Language (OVAL).
- Documentar todos os eventos de segurança, sua investigação e as medidas tomadas, bem como todas as informações, procedimentos e históricos relevantes;
- Coordenar as ações de investigação e de comunicação, interna e externa, de forma centralizada.

Requisito 2.2: Gerenciamento e análise de eventos e informações de segurança

- Gerenciamento de eventos e informações de segurança (*security information and event management* – SIEM)[18, 19] com implantação e utilização de **ferramenta** especializada, incluindo coleta, consolidação, correlação e análise de registros de eventos (log), fontes de telemetria e dados de segurança, podendo incluir monitoramento, inspeção e análise não intrusiva de ativos;
    - Fornecedores de referência[20, 21]:
        - Líderes: Microsoft, IBM, Splunk, Securonix, Exabeam.
        - Desafiantes e Visionários Próximos: LogRythm, Rapid7, Devo, Gurucul, Sumo Logic.
    - Métricas típicas[22]:
        - Eventos por segundo (EPS); Gigabytes por dia (GB/D).
    - Referência:
        - CIS Controle 08 – Gestão de registro de auditoria;
        - CIS Controle 13 – Monitoramento e defesa da rede;
        - Verizon Incident Classification Patterns[23].
- A solução de gerenciamento e seus serviços devem abranger não só o monitoramento, mas a detecção contínua de ameaças e ataques, agregando inteligência de segurança, incluindo análise comportamental de usuários e entidades (*user and entity behavioral analysis* – UEBA) com inteligência artificial e aprendizado de máquina, identificação autônoma de táticas, técnicas e procedimentos (TTPs) mapeando automaticamente com o framework MITRE ATT&CK;
    - Deve ser eficaz na detecção de ameaças e ataques de ransomware;
    - Deve ser capaz de detectar no mínimo as seguintes ameaças de identidade[24]: *password spray*, força bruta, varredura de credenciais, *golden ticket*, *pass-the-hash*, atividade não usual/atípica de usuário, elevação de privilégios, movimentação lateral;
    - Deve ser capaz de produzir e coletar informações de telemetria de tráfego de rede (no mínimo ao nível dos data centers centrais) e de *endpoints* (em especial estações de trabalho e servidores, físicos e virtualizados);
    - Deve ser capaz de coletar logs e informações de telemetria em serviços em nuvem pública de software (SaaS), plataforma (PaaS) e infraestrutura (IaaS), via integração por APIs, protocolos ou agentes que sejam providos e homologados no mínimo para os

[17] Gartner. SOAR: Assessing Readiness Through Use-Case Analysis, 10/03/2020, revisado em 05/10/2021, ID G00464879, por Eric Ahlm.
[18] Gartner. A Guidance Framework for Architecting and Deploying a Modern SIEM Solution, 21/03/2023, ID G00783754, por Kevin Schmidt.
[19] Gartner. Market Guide for Managed SIEM Services, 17/08/2022, ID G00756810, por Al Price, John Collins, Andrew Davies, Mitchell Schneider, Angel Berrios.
[20] Gartner. Magic Quadrant for Security Information and Event Management, 10/10/2022, ID G00755317, por Pete Shoard, Andrew Davies, Mitchell Schneider.
[21] Forrester. The Forrester Wave™: Security Analytics Platform Providers, Q4 2020. Reprodução em Microsoft Security blog, 01/12/2020.
[22] Logpoint. Simple SIEM sizing for everyone – Try our SIEM sizing calculator, 15/01/2019, em https://www.logpoint.com/en/blog/logpoint-siem-sizing-calculator/ e https://siemsizingcalculator.logpoint.com/, acessado em 28/11/2022.
[23] Verizon. Data Breach Investigations Report (DBIR), https://www.verizon.com/business/resources/reports/dbir/, 2022.
[24] Gartner. Enhance Your Cyberattack Preparedness with Identity Threat Detection and Response, 20/10/2022, ID G00765882, por Henrique Teixeira, Peter Firstbrook, Ant Allan, Rebecca Archambault.

seguintes provedores: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud.

- Tratar eventos e alertas em um fluxo de refinamento, através de categorização e priorização, análise crítica, investigação, *threat hunting*, *threat research*, enriquecimento de informações e análises, inteligência de ameaças (*threat intelligence*) estratégica, tática e operacional, e validação, identificando atividades anômalas e, dentre essas, candidatos a incidentes;
- Deve incluir capacidades de integração nativa com ferramentas de proteção, detecção e resposta de endpoints (*endpoint protection platforms* – EPP e *endpoint detection and response* – EDR), incluindo a atual do Tribunal – Broadcom Symantec Endpoint Security (SES)[25,26];
- Prestar apoio técnico e consultivo à configuração da geração adequada de logs e de informações de telemetria nos ativos de TIC de origem relevantes.

Requisito 2.3: Orquestração, automação e resposta (SOAR)

- Gerenciamento, análise, orquestração e automação[27] de políticas, posturas, casos de uso e playbooks com capacidade de resposta autônoma e aplicação próxima a tempo-real, com **ferramenta** de Orquestração, Automação e Resposta de Segurança (*security orchestration, automation and response* – SOAR)[28, 29]; deve ser do mesmo fabricante do SIEM ou totalmente e nativamente integrado ao SIEM, com integração nativa com os diversos ativos e recursos de infraestrutura e segurança de TIC e capacidade de integrar, consolidar, agregar e correlacionar também todas as informações oriundas de outras fontes de telemetria disponíveis;
    - Fornecedores de referência:
        - Que também são fornecedores de referência em SIEM: Exabeam, Gurucul, IBM, Logpoint, LogRythm, ManageEngine, Microsoft, Rapid7, Securonix, Splunk, Sumo Logic (antes DFLabs), Fortinet (antes CyberSponse), Micro Focus (ATAR Labs). Dos fornecedores no Quadrante 2022 Gartner para SIEM, apenas Devo, Elastic e Huawei não são listados por Gartner e/ou Forrester em SOAR.
        - Outros, que tem um portfólio de security analytics: Anomali, Cisco, Cyware, EclecticIQ, Honeycomb, Logsign, NSFOCUS, Palo Alto Networks, QI-ANXIN, Revelstoke, ServiceNow.
        - Outros, pure play ou threat intelligence: D3 Security, DTonomy, LogicHub, Securaa, Shuffle, Siemplify (Google Cloud), SIRP, Swimlane, ThreatConnect, ThreatQuotient, Tines, Torq.

Requisito 2.4: Proteção contra riscos digitais (DRP)

- Monitoramento de proteção da marca e da reputação institucional na internet, na deep web e na dark web, incluindo redes sociais, serviços de comunicação, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, conteúdo malicioso, vazamentos de dados e ameaças externas, realizando takedown em nome do Tribunal mediante procuração e autorização.
- O monitoramento deve incluir, no mínimo:
    - Marca: Tribunal da Justiça do Estado de Minas Gerais, Tribunal de Justiça do Estado de Minas Gerais, Tribunal de Justiça de Minas Gerais, TJMG, TJ-MG;

[25] Broadcom. Symantec Endpoint Security, https://www.broadcom.com/products/cybersecurity/endpoint#endpoint-security, acessado em 13/12/2022.
[26] Broadcom. Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security, https://knowledge.broadcom.com/external/article/154575 e https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Release-Notes/system-requirements-for-v118544952-d4161e11232.html#v118544952__Windows, acessados em 13/12/2022.
[27] Gartner. How to Successfully Implement Automation for Security Operations, 03/02/2022, ID G00757358, por Eric Ahlm.
[28] Gartner. Market Guide for Security Orchestration, Automation and Response Solutions, 13/06/2022, ID G00735883, por Craig Lawson, Al Price.
[29] Forrester. Now Tech: Security Orchestration, Automation, And Response (SOAR), Q2 2022 - Forrester's Overview Of 31 SOAR Providers, 14/04/2022, por Allie Mellen.

  - Subdomínios mais acessados: *.tjmg.jus.br (www, rede, pje, pe, webmail, sei etc.);
  - Perfis oficiais em redes sociais: YouTube @TJMGOficial e @tvtjminas, Instagram TJMGoficial, Facebook TJMGoficial, Twitter tjmgoficial, Flickr tjmg_oficial etc.;
  - Lista VIP de identidades e credenciais.
- As fontes de monitoramento devem incluir, no mínimo:
  - Sites e serviços na internet (aberta ou superficial), na deep web (internet profunda) e na dark web (internet obscura);
  - Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs;
  - Perfis e comunidades em redes sociais e plataformas de mídias sociais: Facebook, Instagram, YouTube, LinkedIn, Twitter, YouTube, TikTok, Flickr, SnapChat, Pinterest;
  - Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns: WhatsApp, Telegram, Signal, Discord, Reddit, Quora;
  - Repositórios e serviços de conteúdo e informação de grande abrangência: Github, Scribd, Reclame Aqui;
  - Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para determinada plataforma de sistema operacional): Microsoft Store (Windows), Google Play (Android), Apple App Store (iOS/iPadOS), Samsung Galaxy Store (Android), Amazon Appstore (Android), F-Droid (Android).
- O serviço deve identificar, no mínimo:
  - Fraudes, phishing e outros tipos de golpes, conteúdo malicioso e ameaças relacionadas;
  - Réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou identidade visual institucionais do Tribunal;
  - Typosquatting (variações de nome, permutações de caracteres e outras variantes visando erros comuns de digitação) e variações ilegítimas ou maliciosas de domínio, marca institucional e outros nomes objeto do monitoramento;
  - Vazamento de dados e informações de segurança e institucionais sensíveis;
  - Reconhecimento e análise de texto em imagens (OCR).
- Monitoramento de ameaças globais e com foco em Brasil, Governo e Judiciário.

Necessidade 3: Gestão de vulnerabilidades e testes de cibersegurança.

Requisito 3.1: Gestão contínua de vulnerabilidades e de exposição a ameaças baseada em riscos

- Gestão contínua de vulnerabilidades e de exposição a ameaças[30, 31, 32, 33, 34, 35], de forma proativa e recorrente, baseada na identificação, avaliação, categorização, priorização, e tratamento e análise crítica de vulnerabilidades e riscos de segurança de ativos corporativos de TIC, gerenciamento e análise de exposição a ameaças e da superfície de ataque interna e externa, com utilização de **ferramenta** especializada para gerenciamento, varredura e avaliação de vulnerabilidades e de configuração segura com análise e priorização do risco cibernético;

[30] Gartner. Implement a Continuous Threat Exposure Management (CTEM) Program, 21/07/2022, ID G00763954, por Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider.
[31] Gartner. A Guidance Framework for Developing and Implementing Vulnerability Management, 24/10/2022, ID G00773547, por Steve Santos.
[32] Gartner. The Top 5 Elements of Effective Vulnerability Management, 23/09/2022, ID G00775767, por Jonathan Nunez.
[33] Forrester. The Forrester Wave™: Vulnerability Risk Management, Q4 2019.
[34] Gartner. Market Guide for Vulnerability Assessment, 25/06/2021, ID G00746908, por Shilpi Handa, Craig Lawson, Mitchell Schneider. "A receita no mercado VA está concentrada em poucos fornecedores, com uma grande porcentagem indo para três deles (Qualys, Rapid7 e Tenable)."
[35] Gartner. Solution Comparison for SaaS-Based Vulnerability Assessment Tools, 13/12/2019, ID G00407253, por Anna Belak, Sushil Aryal, Augusto Barros.

- Deve realizar a descoberta e a identificação de ativos e suas configurações quanto a critérios de segurança, conformidade e aderência a normas, frameworks, posturas e bases de conhecimento; bem como estabelecer linhas de base para os ativos no ambiente de TIC de forma a rastrear e identificar mudanças de estado;
- Deve ter capacidade de avaliação de configuração segura (SCA) remota[36] totalmente integrada na solução de avaliação de vulnerabilidades;
- Deve abranger amplamente ativos corporativos de TIC: dispositivos de usuário final (estações de trabalho e periféricos), inclusive portáteis e móveis, dispositivos de rede, dispositivos inteligentes conectados à rede (como relógios de ponto eletrônico e outros de internet das coisas - IoT), servidores, contêineres, sistemas operacionais, serviços e aplicações em rede, bem como ativos e postura de segurança em nuvem;
- Devem ser realizadas varreduras automatizadas de vulnerabilidade completas em ativos corporativos internos e externos, com periodicidade mínima trimestral e repetição das varreduras após aplicação de atualizações, patches e outras salvaguardas e remediações, incluindo varreduras autenticadas e não autenticadas, com compatibilidade no mínimo com o protocolo Security Content Automation Protocol – SCAP; quando devidamente calibradas, as varreduras automatizadas por agentes e da rede externa devem objetivar a periodicidade diária, e as varreduras da rede interna devem objetivar a periodicidade mensal ou quinzenal, levando em consideração os ciclos de gestão de patches e atualizações e impactos no desempenho, disponibilidade e tráfego dos ativos;
- Deve incluir tecnologia de priorização de vulnerabilidades (VPT) baseada em risco amplamente adaptável, levando em conta severidade das vulnerabilidades, criticidade dos ativos e serviços suportados, e contexto de ameaças (existência e atividade de exploits).
- Fornecedores de referência:
  - Líderes de mercado: Tenable (destaque), Rapid7, Qualys.
  - Líder de mercado – VPT: Ivanti (RiskSense).
- Métrica típica:
  - Quantidade de ativos monitorados.
- Referências:
  - CIS Controle 07 – Gestão contínua de vulnerabilidades;
  - Portaria CNJ nº 162/2021, Anexo IV: Manual de Referência – Proteção de Infraestruturas Críticas de TIC, Checklist de controles mínimos recomendados, tópico 3: Gerenciamento Contínuo de Vulnerabilidade;
  - ABNT ISO/IEC 27005:2019 - Gestão de riscos de segurança da informação (e sua atualização 2022/2023);
  - NIST Special Publication (SP) 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;
  - CIS RAM - CIS Risk Assessment Method (RAM) v2.1;
  - Common Vulnerability Scoring System (CVSS) v3.0 ou v3.1;
  - NIST CVSS Calculators.

- Agregação de recursos de inteligência de ameaças (*threat intelligence*) para rastreamento do uso ativo e priorização de vulnerabilidades, incluindo fontes estratégicas (relatórios, bases de conhecimento, *feeds*, fóruns e comunidades abertos, da Deep e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos – TTPs) e operacionais (correlação com indicadores de comprometimento – IOCs), do fabricante da ferramenta combinada com fontes abertas e da contratada;
  - Referência:
    - MITRE ATT&CK framework;
    - Exploit Database da Offensive Security;
    - MISP Threat Sharing;
    - OASIS Open Structured Threat Information eXchange (STIX) e Trusted Automated eXchange of Indicator Information (TAXII).

[36] Gartner. Best Practices for Secure Policy Configuration Assessment, 28/10/2016, ID G00316134, por Oliver Rochford, Prateek Bhajanka.

- Acompanhamento de alertas de segurança, atualizações de segurança, referenciais de vulnerabilidades e melhores práticas de higienização de segurança e de *hardening* para ativos de TIC, incluindo, mas não se limitando a:
    - NIST National Vulnerability Database (NVD), MITRE Common Vulnerabilities and Exposures (CVE), NIST Official Common Platform Enumeration (CPE), MITRE Common Weakness Enumeration (CWE), OWASP Top 10, CIS Benchmarks;
    - Repositórios e centros de segurança dos principais fornecedores/fabricantes de tecnologia aplicáveis aos ativos de TIC do Tribunal, contemplando no mínimo: Microsoft, Oracle, Google, Red Hat, Dell/EMC, HP/Aruba, Check Point, F5 Networks, Broadcom/Symantec, VMware, Micro Focus, Commvault, Cisco, Mozilla, Adobe.
    - Referência:
        - CIS Controle 04 – Configuração segura de ativos corporativos e software.

Requisito 3.2: Testes de segurança automatizados (BAS)

- Planejamento, execução, análise e relatório de testes automatizados continuados de segurança[37] com **ferramenta** de simulação de brechas e ataques (*breach and attack simulation* – BAS)[38];
    - Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno; e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows;
    - As simulações devem garantir ambiente controlado e sem impacto nocivo real;
    - Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos.
    - Fornecedores de referência[39,40]:
        - Picus Security, Cymulate, AttackIQ, SafeBreach, XM Cyber, Pentera, Keysight, Mandiant.
    - Métricas típicas:
        - Quantidade de ativos-alvo ou golden images (templates de imagens de ambiente/configuração);
        - Seguimento testado.

Requisito 3.3: Testes de invasão (Pentest)

- Planejamento, execução, análise e relatório/apresentação de resultados de **testes de invasão**, com periodicidade estimada semestral, com planejamento de objetivos e escopo, definição de atuação black box, gray box, ou white box.
    - Referências:
        - CIS Controle 18 – Testes de invasão;
        - MITRE ATT&CK framework;
        - Open Source Security Testing Methodology Manual (OSSTMM 3) do ISECOM;
        - PTES - Penetration Test Execution Standard;
        - CHECK do National Cyber Security Centre (NCSC) do Reino Unido;
        - Curso Penetration Testing with Kali Linux (PWK/PEN-200) e certificação Offensive Security Certified Professional (OSCP) da Offensive Security;
        - OWASP Web Security Testing Guide.

[37] Gartner. Using Security Testing to Grow and Evolve Your Security Operations, 29/04/2022, ID G00763253, por Eric Ahlm.
[38] Gartner. Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?, 26/08/2022, ID G00760272, por Mitchell Schneider, Jeremy D'Hoinne, Craig Lawson.
[39] Comparitech. 6 Best Breach and Attack Simulation (BAS) Tools, por Amakiri Welekwe, 05/08/2022, em https://www.comparitech.com/net-admin/best-bas-tools/ acessado em 28/11/2022.
[40] Gartner. Fast Answer: What should I know about Breach and Attack Simulation?, https://www.gartner.com/fast-answer/tech/fec54061-385d-31a5-ae1a-91fca044b2fa, acessado em mar/2023.

Necessidade 4: Adotar medidas iniciais para melhoria da gestão de identidade e acesso.

Requisito 4.1: Diagnóstico e avaliação de governança de identidade e gestão de acessos

- Identificação e mapeamento:
    - Das fontes de identidade e vínculos de pessoas, como sistemas de gestão de recursos humanos, sistemas de contratos e pessoal terceirizado e outros cadastros e controles de pessoas físicas, identificando perfis que caracterizam a utilização de recursos computacionais que caracterizam a situação de usuários de TIC;
    - Dos eventos e situações que caracterizam início, alteração, suspensão e término de vínculos que façam jus à necessidades de provisionamento e desprovisionamento de perfis e atribuições;
    - Dos processos de cadastramento e alteração de usuários e acessos e dos atendimentos de usuários de TIC, self-service e intermediados pelas equipes de atendimento e suporte;
    - Das características detalhadas dos repositórios de informações e recursos de credenciais de acesso, autenticação e autorização: Microsoft Active Directory, OpenLDAP, KeyCloak, Oracle Database Server;
    - Dos requisitos e das necessidades de governança e gestão de identidade (IGA) do Tribunal;
    - Dos requisitos e das necessidades do Tribunal em gestão de credenciais, autenticação e autorização, incluindo políticas de senha, mecanismos de múltiplo fator de autenticação (MFA/2FA), gestão de acessos e autenticação em nuvem, teletrabalho, outros acessos remotos e interação com atores externos, políticas de acesso baseadas em confiança-zero (*zero trust*) e outras melhores práticas aplicáveis.
- Diagnóstico, análise de maturidade e de gap e proposição de estratégias e planos de evolução do cenário e de adoção de políticas, processos, práticas e tecnologias na governança e administração de identidade (IGA) e na gestão de acessos do Tribunal.

4.1.2 Requisitos de implantação e capacitação

Como preparação para a implantação dos serviços, é necessário levantamento e avaliação detalhada do ambiente de TIC e da cibersegurança do Tribunal.

A implantação deve ser tratada como um projeto, devidamente acompanhada por um gerente técnico de conta. Durante a implantação dos serviços, dada sua grande abrangência e complexidade, é necessário também que a equipe técnica da DIRFOR mais diretamente envolvida na gestão e operações de cibersegurança e na execução dos serviços pretendidos seja capacitada, de forma a obter uma visão geral e compreensão dos principais componentes que farão parte das soluções.

Necessidade 1: Levantamento e avaliação inicial da infraestrutura e dos ativos de TIC.

- Além do diagnóstico e avaliação inicial de situação e maturidade previstos nos requisitos de negócio, para a implantação deve ser feito levantamento, descoberta, higienização e consolidação do mapeamento dos ativos de hardware e software de TIC e seus controles, complementados por entrevistas técnico-gerenciais, formando uma visão precisa e detalhada da superfície de ataque do Tribunal, incluindo:
    - Arquitetura geral da infraestrutura de TIC;
    - Estrutura física de data center e salas de dados;

- Ativos de hardware de infraestrutura de processamento, armazenamento, rede e comunicação de dados, endpoints (dispositivos de usuário final como estações de trabalho, servidores e periféricos) e dispositivos inteligentes (como multifuncionais, relógios de ponto eletrônico e outros de internet das coisas - IoT) conectados à infraestrutura fisicamente, virtualmente, remotamente e em ambiente de nuvem;
- Ativos de software de sistemas corporativos, aplicativos, utilitários e sistemas operacionais, contêineres e ambientes virtualizados;
- Validação do que consta atualmente no Universal CMDB do Tribunal.
- Referências:
  - CIS Controle 01 – Inventário e controle de ativos corporativos;
  - CIS Controle 02 – Inventário e controle de ativos de software.

Necessidade 2: Capacitação e transferência de conhecimento.

- Treinamento presencial para até 20 pessoas da equipe técnica de informática sobre as metodologias, processos, tecnologias e recursos que estão sendo implantados nas soluções para os serviços contratados, com carga horária mínima de 20 horas/aula, sendo no máximo 4 horas/aula por dia, e fornecimento de material de referência em formato digital.

Necessidade 3: Mobilização e implantação.

- Alocação de Gerente técnico de conta (*technical account manager* – TAM) e de Preposto da implantação e das operações;
- Plano de implantação e operação, cronograma detalhado e relatórios de acompanhamento;
- Mobilização, instalação e adequação inicial de recursos (pessoas, processos e tecnologias);
- Fornecer ampla documentação e treinamento para as ferramentas e soluções implantadas, incluindo configurações e ajustes, para a equipe técnica do Tribunal.

4.1.3 Requisitos legais

O projeto está alinhado à Resolução CNJ nº 370/2021, art. 2º, inciso I, alínea c: Aprimorar a Segurança da Informação e a Gestão de Dados, em processos internos da ENTIC-JUD.

Está especialmente alinhado à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ nº 396/2021, contemplando (de forma mais ampla) ou contribuindo (de forma mais limitada ou parcial) para vários comandos relativos a medidas para elevar o nível de segurança das infraestruturas críticas, conforme a seguir.

Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

- I - estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão; (contribui)
- II - instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR); (contempla)

- III - elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa; (contempla)
- IV - utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança; (contempla)
- V - utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet; (contempla)
- VII - elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e celulares; (contribui)
- X - realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos; (contempla)
- XI - realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; (contempla)

Art. 26. Todos os órgãos do Poder Judiciário deverão adotar e seguir:

- I - Protocolo – Prevenção de Incidentes Cibernéticos do Poder Judiciário; (contempla)
- II - Protocolo – Gerenciamento de Crises Cibernéticas do Poder Judiciário; (contempla)
- III - Protocolo – Investigação para Ilícitos Cibernéticos do Poder Judiciário; (contribui)
- IV - Manual de Referência – Proteção de Infraestruturas Críticas de TIC; (contribui)
- V - Manual de referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital; (contribui)
- VI - Manual de Referência – Gestão de Identidade e de Controle de Acessos; (contribui)
- VII - Manual de Referência – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário. (contribui)

Art. 29. Cada tribunal deverá implementar a gestão de usuários de sistemas composta de:

- I – gerenciamento de identidades; (contribui)
- II – gerenciamento de acessos; e (contribui)
- III – gerenciamento de privilégios. (contempla)

Também está alinhado à Resolução CNJ nº 363/2021, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) a serem adotadas pelos tribunais, em especial seu art. 1º, inciso XI, na medida em que as necessidades aqui identificadas visam estabelecer controles e procedimentos de segurança para proteger as informações em meio digital, inclusive dados pessoais, bem como tratamento e resposta a incidentes cibernéticos.

4.1.4 Requisitos de sustentação

Necessidade 1: Sustentação de todas as ferramentas fornecidas.

Todas as ferramentas fornecidas como parte das soluções devem contar com serviços plenos de sustentação, conforme a seguir.

- A sustentação, administração, operação, suporte técnico e atualização das ferramentas fornecidas pela contratada, como SIEM, SOAR, VA, BAS e qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos serão serviços de natureza continuada de responsabilidade da contratada;
- Para cada uma delas, devem ser fornecidos os serviços de suporte técnico e de atualização oficiais e prioritários do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços envolvidos, que devem estar contratados e disponíveis a partir da implantação da respectiva ferramenta e, daí em diante, durante toda a vigência do contrato;
- A contratada deve comprovar um nível de parceria oficial amplo e prioritário junto ao fabricante, tal que permita amplo e irrestrito acesso aos recursos e serviços de apoio técnico e de acesso à plenitude de capacidades e efetividade das ferramentas, prestados diretamente pelo fabricante, como centros e laboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis;
- As ferramentas que forem de uso exclusivo do Tribunal, ou que sejam assim demandadas pelo modelo de negócios do fabricante, devem ser devidamente licenciadas ou subscritas em nome do TJMG, devendo a contratada apresentar a devida comprovação para que sejam iniciados os pagamentos dos respectivos itens de serviço.

4.1.5 Requisitos temporais

Os serviços necessários de natureza continuada são de grande complexidade e abrangência, de forma que é esperado um período em torno de 90 dias para a implantação inicial de todos eles e de vários meses para que os processos, recursos e atividades envolvidos sejam gradativa e continuamente estabilizados, ajustados e refinados. Por outro lado, o ineditismo dos serviços, seu impacto cultural e operacional na organização e a intensa e acelerada evolução atual do mercado de cibersegurança levam a consideráveis níveis de incerteza sobre a adequação, eficácia e eficiência da execução dos serviços no longo prazo. Desta forma, quando a execução dos serviços estiver em sua plenitude, o Tribunal precisará de tempo considerável para absorver e avaliar adequadamente os serviços, tecnologias e processos e seus resultados, bem como planejar e executar próximos passos de continuidade ininterrupta, seja por prorrogação ou nova contratação. Além disso, antes do encerramento do contrato, deve haver um prazo de pelo menos três meses para transição contratual. Por todo o exposto, um prazo inicial de 36 meses, prorrogáveis dentro dos limites legais, se justifica.

- Os serviços de execução continuada devem ser contratados pelo prazo inicial de 36 meses, podendo haver prorrogação até o limite legal.
- Prazos máximos na execução dos serviços:
    - O plano de implantação e operação deve ser apresentado em até 10 dias corridos após a assinatura do contrato.
    - O serviço de Levantamento e avaliação inicial da infraestrutura e dos ativos de TIC e o primeiro diagnóstico e avaliação de gap (situação e lacunas) e maturidade dos Serviços

estratégicos de governança, risco e conformidade (GRC) devem ser entregues em no máximo 6 semanas após a assinatura do contrato.

- O prazo máximo para operacionalização do serviço de Centro de operações de segurança (SOC), equipe de tratamento e resposta a incidentes (ETIR) e gerenciamento e análise de eventos e informações de segurança (SIEM) deve ser de três meses, a partir da assinatura do contrato.

- Dada a vigência das obrigações da Resolução CNJ nº 396/2021 e a urgência dos riscos e ameaças atuais de cibersegurança, é esperado que os serviços sejam contratados até o final de 2023 e que sua implantação e execução ocorra a partir de 2024.

4.1.6 Requisitos de segurança da informação e proteção de dados pessoais

- Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto e informação de que tomar conhecimento em razão da execução do objeto do Contrato.
- Providenciar assinatura do Termo de Sigilo e Confidencialidade, conforme modelo anexo, pelo representante legal da empresa.

4.2 Identificação das necessidades tecnológicas

- Os serviços continuados remotos devem ser executados em regime 24 × 7, mantidos em SOC com infraestrutura de alta disponibilidade e com certificação ISO 27001.
- Deve também haver ambiente redundante de recuperação de desastre (DR) apto a assumir plena e integralmente a execução dos serviços sob emergência; situado em cidade e região metropolitana distinta, como geo-redundância para mitigar o risco de perda total dos dados e interrupção dos serviços em caso de desastres naturais, falhas de energia ou outros eventos adversos.
- As ferramentas utilizadas devem ser providas em infraestrutura própria da contratada ou do fabricante, ou em ambiente de computação em nuvem pública adequado. Se houver a necessidade de implantação de controladores, concentradores, coletores, sensores, agentes, *appliances* e qualquer outro recurso de hardware e software local na infraestrutura interna do Tribunal, a contratada deve fornecer e sustentar todos os recursos necessários e ser responsável pelo seu fornecimento, implantação, instalação, configuração, sustentação, atualização, administração e operação, sem custo adicional.
- Toda a comunicação de dados entre a infraestrutura interna do Tribunal e a infraestrutura da contratada deve ser criptografada e otimizada de forma a não introduzir latência inadequada ou óbice ao pleno desempenho, disponibilidade e eficácia da execução dos serviços e seus resultados.
- Todos os serviços, ferramentas, controles e camadas de segurança devem ser integrados e consolidados em uma arquitetura unificada e harmonicamente orquestrada e gerida, provendo como resultado uma camada final de centralização, com um ou mais painéis (dashboards) técnico-operacionais e um painel estratégico-gerencial.

4.3 Demais requisitos necessários e suficientes à escolha da solução de TIC

Dado o ineditismo, complexidade e abrangência dos serviços, podem ao longo do tempo surgir necessidades correlatas imprevistas nos requisitos, mas pertinentes ao objeto global. Desta forma, é pertinente prever serviços técnicos especializados conforme a seguir.

Necessidade 1: Serviços técnicos especializados, sob demanda

- Execução de serviços técnicos especializados para atividades não previstas no escopo anteriormente definido, a serem demandados, aprovados e executados sob demanda, mediante ordem de serviço (OS), na forma de um banco de horas técnicas anual.

Necessidade 2: Equipe dedicada presencial

- Deve haver uma equipe dedicada de pessoas-chave, alocada em tempo integral nas dependências do Tribunal em Belo Horizonte, em regime presencial, apta a atuar nos serviços de Governança e gestão de segurança de TIC; Monitoramento, detecção e resposta gerenciados de segurança; Gestão de vulnerabilidades e ameaças e testes de segurança; abrangendo as atividades críticas, sensíveis e as que envolvem entendimento, interação e transferência de conhecimento frequente com o ambiente e as equipes do Tribunal.
    - A equipe dedicada deve contemplar no mínimo 5 (cinco) pessoas, sendo no mínimo 2 (dois) com perfil nível sênior e 3 (três) com perfil nível pleno (qualificações, experiência e certificações a serem detalhadas);
    - A equipe dedicada atuará em horário comercial de acordo com o calendário de dias úteis do Tribunal para a comarca de Belo Horizonte, disponível no Portal do TJMG, mas poderá atuar, sob demanda a critério do Tribunal e mediante planejamento prévio, em dias não úteis e horários não comerciais, para atividades urgentes e inadiáveis e atividades que requeiram execução em dias e horários de menor impacto para a disponibilidade e a continuidade dos serviços de TIC do Tribunal.

Necessidade 3: Integrações, alinhamento e limites de responsabilidade

- Equipes de sustentação de infraestrutura, operações e sistemas: escalar requisições e incidentes de segurança, quando envolver equipes internas ou contratos de apoio e outros serviços específicos existentes para os ativos de TIC envolvidos;
- Serviços e processos de monitoramento da infraestrutura e sistemas de TIC (NOC): orientar a geração e encaminhamento de logs úteis ao syslog e SIEM e garantir a comunicação bilateral de eventos de segurança que afetem disponibilidade e desempenho;
- Gestão de serviços de TIC, incluindo a Central de Serviços: nas requisições, incidentes e mudanças, adotar integralmente os processos, integrar (via API ou serviços web) com ou utilizar a ferramenta de ITSM, realizar a comunicação bilateral com a Central de Serviços de TI para alertas, requisições e incidentes;
- Unidades e processos institucionais de governança e conformidade, de segurança institucional, de segurança da informação e de privacidade e proteção de dados pessoais;
- Coordenação e cooperação com ETIRs de outros órgãos públicos e privados.

5 ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Unidades e quantidades dos serviços pretendidos:

- Os serviços continuados devem ser dimensionados e pagos por mês, englobando todos os serviços, ferramentas e recursos necessários, para a quantidade inicial de 36 meses.
- Os diagnósticos e avaliações avulsos (na Implantação e na Identidade e Acesso), bem como a capacitação (na Implantação), serão mensurados por empreitada, 1 unidade cada.
- Os testes de invasão (pentest) devem ser providos como serviço de natureza continuada, porém para uso sob demanda mediante ordem de serviço; são estimados para serem realizados semestralmente, em conformidade com o art. 11, inciso X da Resolução CNJ nº 396/2021; para o prazo de 36 meses, portanto, está prevista a quantidade de 6 execuções.
- Os serviços técnicos especializados devem ser providos como serviço de natureza continuada, porém para uso sob demanda mediante ordem de serviço, como um banco de horas técnicas anual; a estimativa de quantidade de horas técnicas para o prazo de 36 meses é 3.600, suficientes para até 6,8 homens-mês/ano, ou uma média de até 100 homens-hora/mês.

Nesta forma, os serviços atendem integralmente a demanda atual.

6 REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução inviável 1: Evoluir a equipe e a estrutura internas

No âmbito desta solução, a proposta seria prover serviços de cibersegurança pela alocação e capacitação de equipe interna e aquisição e integração de soluções de mercado para as ferramentas e tecnologias necessárias, incluindo hardware (equipamentos) e software (licenças ou subscrições), serviços de implantação, garantia, atualização e suporte técnico. Além disso, as soluções deveriam ser mantidas em infraestrutura e operação de alta disponibilidade 24 × 7.

Esta solução atende parcialmente aos requisitos listados no item 3 deste ETP.

Justificativa da inviabilidade:

Mesmo com os esforços da DIRFOR, esta diretoria possui uma capacidade limitada de pessoal — não só em quantidade e especialização, mas em experiência adequada, o que por si só já inviabilizaria a alocação e capacitação de equipe interna adequada em tempo hábil. A formação profissional especializada e proficiência de analistas e gerentes em cibersegurança em geral consome de três a cinco anos. Há que se considerar também que a jornada de trabalho e demais instrumentos de recursos humanos atualmente disponíveis para a execução de atividades continuamente em regime 24 × 7 por serventuários ainda são um desafio não equacionado pelo Tribunal. Além disso, a contratação à parte e integração de produtos e serviços relativos às ferramentas e tecnologias necessárias é de uma complexidade proibitiva frente à diversidade e constante evolução do mercado, como se vê em outras soluções inviáveis adiante.

Solução inviável 2: Contratar e implantar um SOC interno

O mercado de provedores de serviços gerenciados de cibersegurança tem oferecido amplamente SOCs próprios remotos, com os devidos controles gerenciais e operacionais para segmentar de forma

segura um ambiente para atender às necessidades de monitoramento, detecção e resposta gerenciados para cada cliente, ao mesmo tempo que permitem compartilhar as instalações físicas e ambientes de alta disponibilidade e redundância para operação 24 × 7 adequadamente, bem como o aproveitamento de especialistas de alta senioridade e especialidade nos diversos aspectos e tecnologias abrangidas, aptos a suprir as necessidades mais avançadas de apoio, suporte e transferência de conhecimento avançados.

Um SOC interno exigiria ao Tribunal dispor e manter uma onerosa infraestrutura e redundância de alta disponibilidade exclusiva. Ainda mais grave, um SOC interno exigiria alocação dedicada de toda ou da maior parte da equipe atuando diretamente na execução das atividades, o que conflita com a atual escassez de profissionais altamente qualificados e experientes neste mercado.

Solução inviável 3: Fazer um parcelamento do objeto tal que separe o fornecimento de ferramentas e tecnologias do fornecimento dos serviços e equipe técnica.

Existe uma grande diversidade e possibilidades distintas de ferramentas e tecnologias que podem compor a solução, com o mercado em plena evolução e consolidação. Por outro lado, todos os provedores de serviços gerenciados de segurança cibernética mantém parceria com diversos fabricantes e fornecedores de tecnologia, bem como já detém experiência, metodologia e estruturação na utilização de um conjunto de tecnologias que atendem à solução pretendida, de forma que se tem muito mais eficiência, integração e, provavelmente, economia de tempo e recursos, se o próprio provedor de serviços fornecer, sustentar e utilizar as ferramentas e tecnologias necessárias.

Além disso, observa-se no mercado atual que praticamente todos os fabricantes têm caminhado para o modelo de fornecimento de software e de tecnologias como serviço, em geral disponibilizados em nuvem e pagos como subscrição e assinatura, o que facilita muito integrá-los no formato e composição de custos de serviços continuados com pagamentos mensais e evita a necessidade de grandes investimentos iniciais em aquisição de equipamentos e licenciamentos perpétuos.

Desta forma, seria inviável, dentro da enorme diversidade e evolução do mercado e agravado por nossa pouca experiência e maturidade em segurança cibernética tentar definir a priori um rol de ferramentas para parcelamento e compor uma complexa integração à parte envolvendo diversos fabricantes, tecnologias e fornecedores distintos. Mais inviável e arriscado ainda seria tratar as ferramentas e tecnologias de forma apartada dos serviços correlatos e da equipe técnica envolvida.

7 ANÁLISE DE SOLUÇÕES POSSÍVEIS

Estudos de mercado dos principais institutos mostram que o mercado de serviços gerenciados de segurança cibernética, em inglês *managed security services* – MSS, está muito consolidado e em franca expansão.

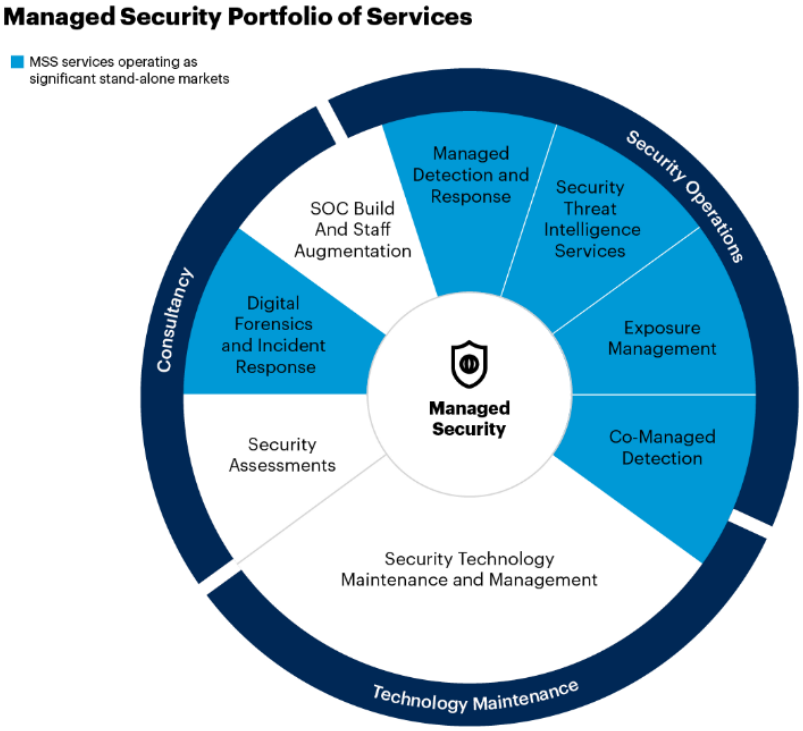
O estudo do Gartner “Market Guide for Managed Security Services”, 16/03/2022, ID G00741325, por Pete Shoard, Mitchell Schneider, John Collins, Al Price, traz a seguintes definições e principais apontamentos sobre esse mercado e seu portfólio de serviços:

Os serviços gerenciados de segurança (MSS) fornecem às organizações uma variedade de serviços operacionais e de gerenciamento específicos para tecnologias de segurança cibernética e da informação e resultados de negócios para segurança. Os recursos incluem monitoramento, detecção e resposta, avaliação e gerenciamento de exposição, bem como consultoria de segurança e implementação de tecnologias de segurança. Os MSSs são entregues em uma variedade de modos, na infraestrutura de nuvem dos provedores, como compromissos consultivos ou por meio de aumento de equipe e no local.

Os provedores de serviços gerenciados de segurança (MSSP) oferecem uma variedade de serviços de segurança cibernética e da informação que variam de provedor para provedor. Essa amplitude de ofertas de serviços oferece ampla escolha, e cada vez mais se sobrepõe aos recursos oferecidos por outros segmentos de mercado.

Os recursos de segurança baseados em software como serviço (SaaS) tiveram precedência para muitos compradores, reduzindo significativamente a necessidade de utilizar um provedor terceirizado distinto para manter as tecnologias de segurança.

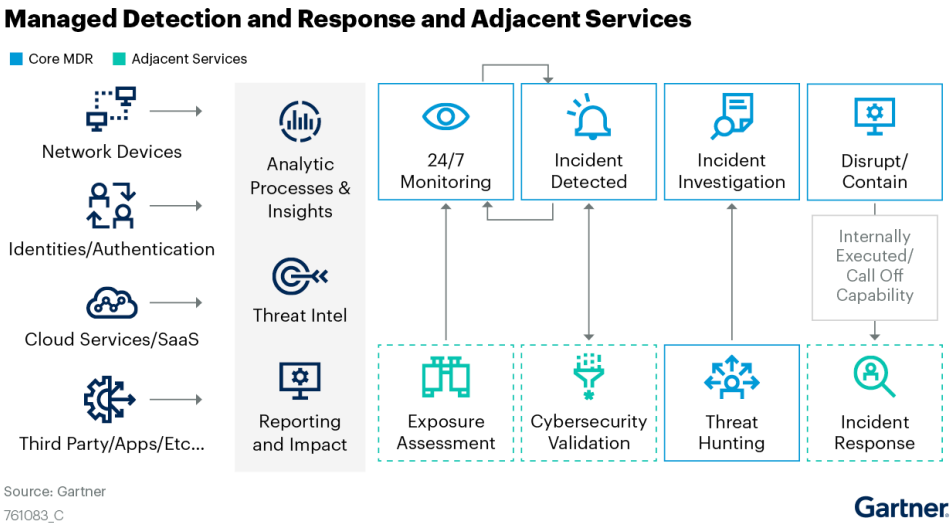
O Gartner prevê como planejamento estratégico que até 2024, 90% dos provedores de segurança gerenciada terão abandonado plataformas de segurança construídas organicamente em favor de soluções disponíveis comercialmente em um modelo SaaS.



Estas análises são confirmadas em estudo similar do Forrester: "The Forrester Wave™: Global Managed Security Services Providers – The 15 Providers That Matter Most and How They Stack Up", 27/07/2020, por Jeff Pollard e Claire O'Malley, https://www.forrester.com/report/The-Forrester-Wave-Global-Managed-Security-Services-Providers-Q3-2020/RES157492.

Outros estudos pesquisados e listados a seguir detalham segmentos desse mercado, como os serviços gerenciados de detecção e resposta (MDR) e o tratamento e resposta a incidentes.

Gartner. "Market Guide for Managed Detection and Response Services", 14/02/2023, ID G00761083, por Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies.

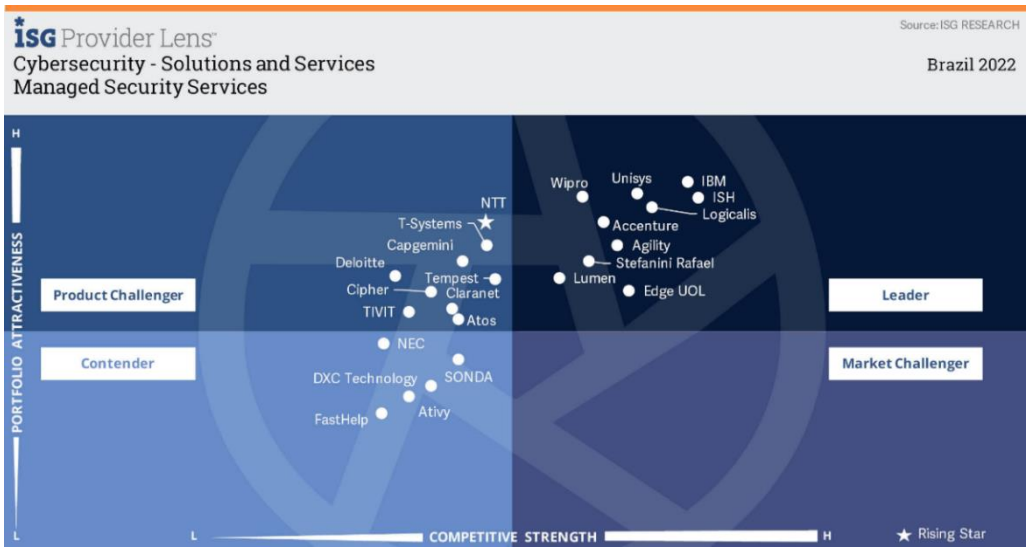


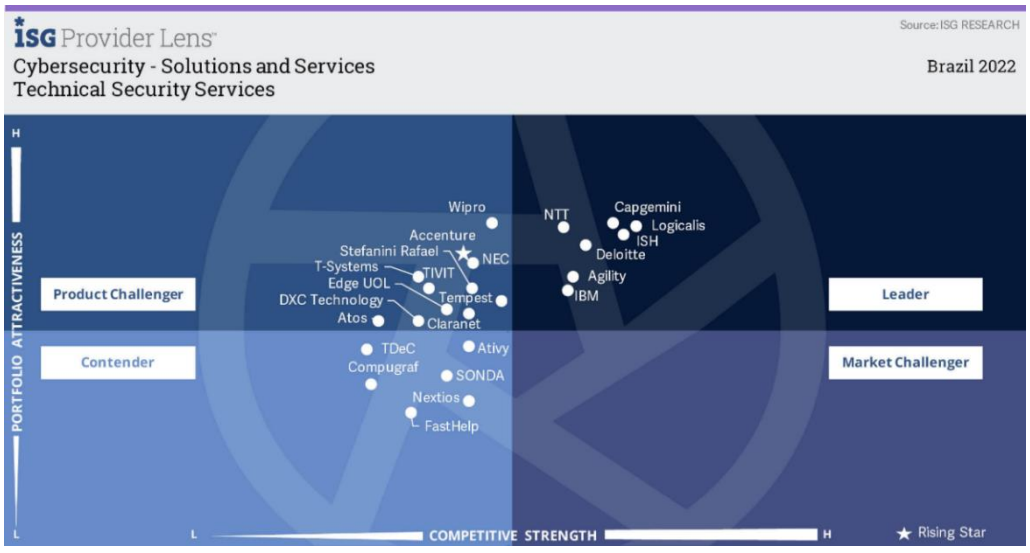
Forrester. “The Forrester Wave™: Managed Detection and Response, Q1 2021 – The 15 Providers That Matter Most and How They Stack Up”, 24/03/2021, por Jeff Pollard, Claire O'Malley. O infográfico a seguir destaca estimativas de horas poupadas por principais atividades (descritas em inglês), em razão da contratação de um provedor de serviços.

Forrester. “The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2022 – The 13 Providers That Matter Most And How They Stack Up”, 28/03/2022, por Jess Burn.

Contudo, provavelmente a referência mais relevante encontrada foi um estudo anual do instituto ISG, que segmenta a análise desse mercado especificamente para o Brasil e confirma que dezenas de empresas tem ampla e sólida atuação nacional como provedores de serviços gerenciados de segurança cibernética, incluindo tanto serviços estratégicos quanto técnicos:

Information Services Group (ISG) Research. “ISG Provider Lens: Cybersecurity - Solutions and Services, 2022, Brasil”, Quadrant Report, julho 2022, por Sérgio Rezende.





Várias destas empresas de serviços em segurança cibernética no estudo do ISG no Brasil aparecem também em estudos de mercado globais/mundiais, como o estudo anual da MSSP Alert, que lista os 250 maiores provedores de serviços gerenciados de segurança cibernética no mundo: “Top 250

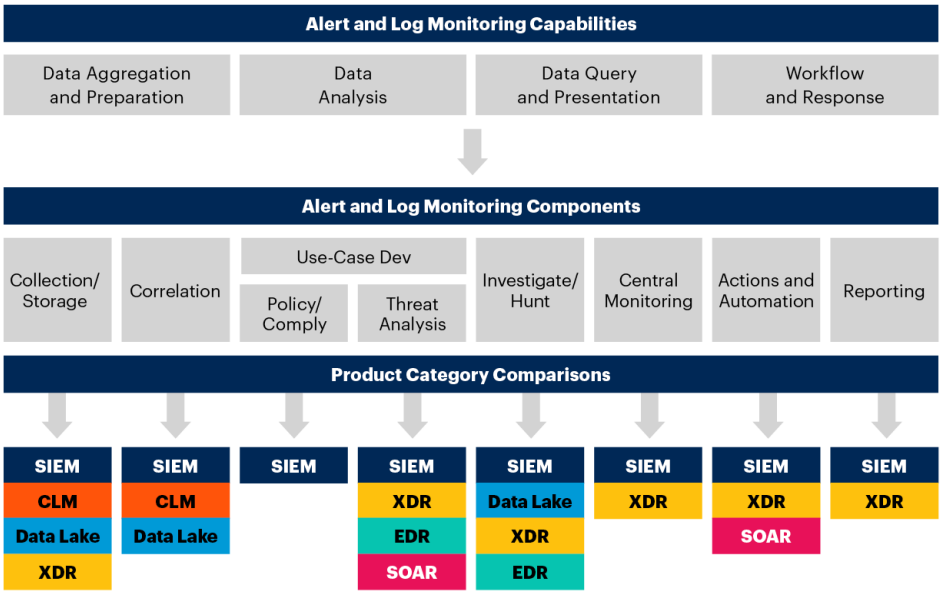
MSSPs Cybersecurity Companies List and Annual Research, 2022", disponível em https://www.msspalert.com/top250/, acessado em fevereiro 2023, e estudos do Gartner e do Forrester sobre serviços gerenciados de cibersegurança.

Com efeito, diversos órgãos públicos têm realizado com sucesso licitações de serviços gerenciados de segurança cibernética, variando em escopo, dada a amplitude e variedade do portfólio de serviços disponíveis no mercado, aqui apontada, e em razão da realidade de cada órgão quanto a seu porte, tamanho, equipe técnico-administrativa, prazos e orçamento disponíveis.

As prospecções de mercado realizadas pelo TJMG com diversas empresas, entre provedores e fabricantes, também confirmaram a existência de boas empresas aptas a prestar os serviços e soluções pretendidas. Todos os provedores relevantes de serviços de cibersegurança têm parcerias comerciais firmadas com dezenas de grandes fabricantes mundiais de tecnologia nos diversos segmentos de segurança cibernética, sendo capazes de fornecer e integrar uma composição de tecnologias e ferramentas que atenda de forma plena as necessidades e requisitos listados no item 3 deste documento, oferecendo competitividade ao certame.

É importante ressaltar que são muitas e complexas as tecnologias envolvidas em serviços gerenciados de segurança cibernética, que tem evoluído e ampliado nos últimos anos, muitas vezes com sobreposição entre elas. Por exemplo, o estudo do Gartner "Is Security Operations Ready for XDR?", 03/11/2021, ID G00735336, por Eric Ahlm e Jon Amato, aborda sobreposições entre categorias de produtos como detecção e resposta estendida (XDR), gerenciamento de eventos e informações de segurança (SIEM) e outras, conforme ilustrado na figura a seguir.

The XDR Overlap to SIEM



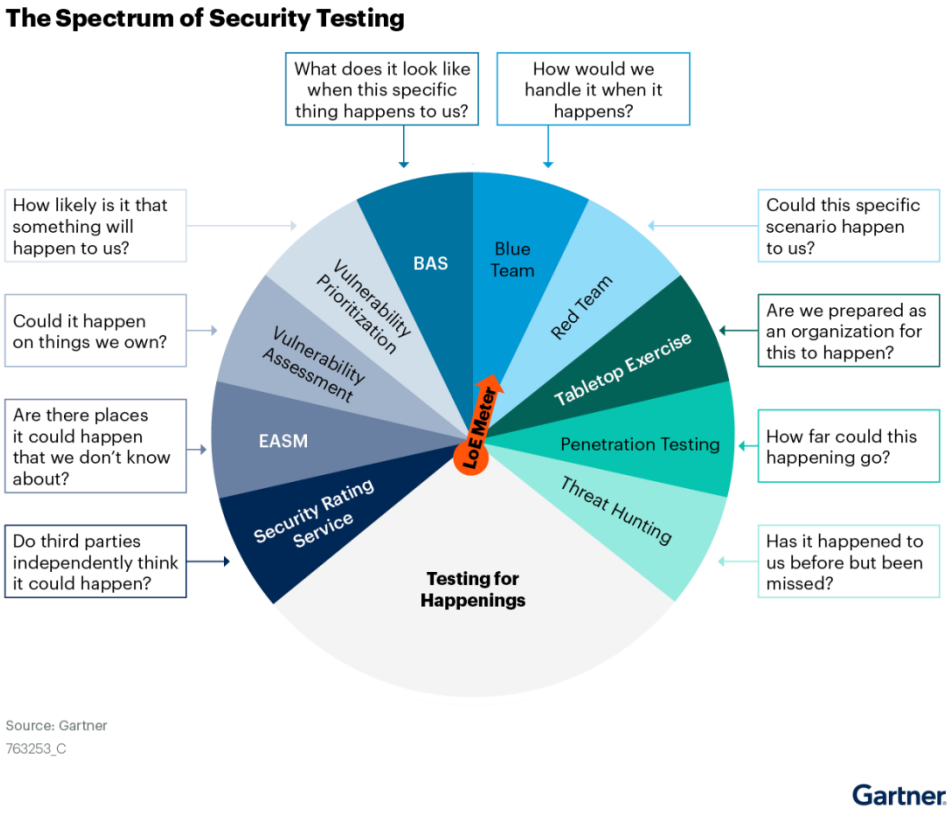
Note: SIEM spans the capabilities to offer more comprehensive monitoring and reporting.
Source: Gartner
735336_C

Gartner

Estas sobreposições e conflitos são também abordados no artigo do Forrester "Introducing The Forrester New Tech: Extended Detection And Response (XDR) — A Battle Between Precedent And Innovation", por Allie Mellen, 02/08/2021, https://www.forrester.com/blogs/introducing-the-

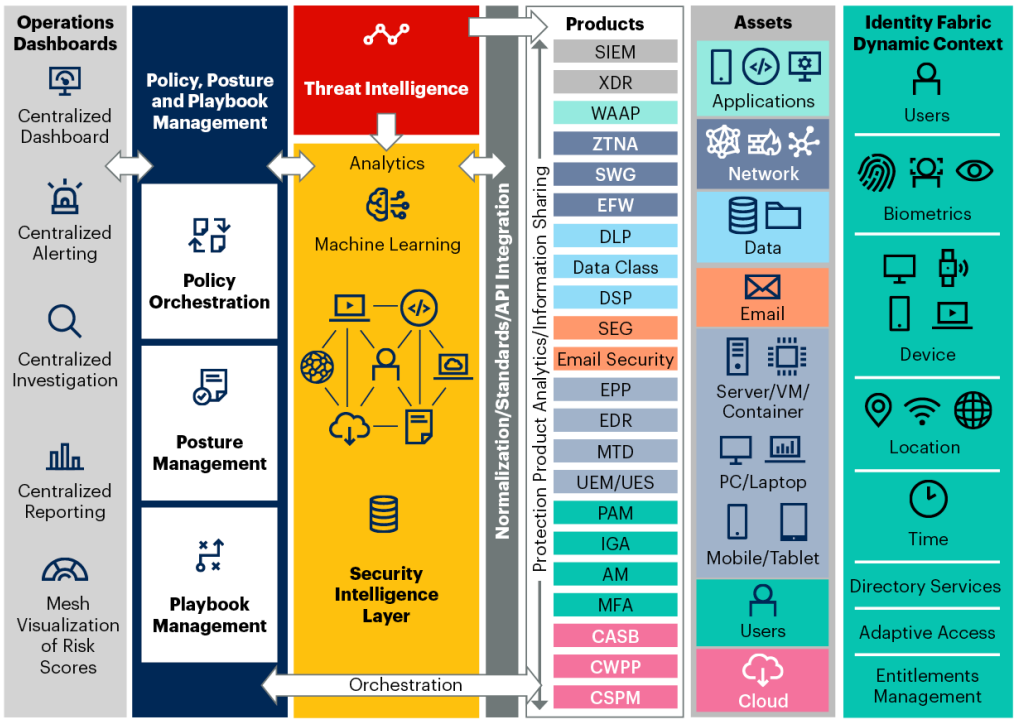
forrester-new-tech-extended-detection-and-response-xdr-a-battle-between-precedent-and-innovation/, acessado em março/2023.

Outro estudo do Gartner, "Using Security Testing to Grow and Evolve Your Security Operations", 29/04/2022, ID G00763253, por Eric Ahlm, aborda o vasto espectro de serviços e tecnologias existentes em gestão de vulnerabilidades e testes de segurança, como se pode ver na figura a seguir.



Portanto, um MSSP terá melhores condições de selecionar, fornecer e integrar um conjunto de tecnologias e ferramentas que melhor atendam ao Tribunal, tanto em termos de adequação como em competitividade comercial, compondo o que o Gartner denomina arquitetura de malha de segurança cibernética (CSMA) no artigo: "The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)", 12/01/2022, ID G00754315, por Patrick Hevesi e Mary Ruddy.

Cybersecurity Mesh Architecture Reference



Source: Gartner
Note: Products included in the diagram are not all of the products that can be included but an example list of possible tools that protect assets
754315_C

Gartner

7.1 Identificação das Soluções

Por todo o exposto, chegou-se ao modelo de solução como se segue.

Id	Descrição da solução (ou cenário)
Única	Contratação de serviços gerenciados de segurança cibernética (*managed security services* - MSS), de natureza continuada, remotos e presenciais, com fornecimento de equipe técnica especializada, ferramentas, processos e transferência de conhecimento.

7.1.1 Fornecedores

Foram prospectadas várias empresas, das quais três mantiveram contatos para o refinamento do escopo até a apresentação de uma proposta preliminar de solução com orçamento:

- ISH Tecnologia: No mercado desde 1996, maior provedor de serviços gerenciados de segurança da América Latina segundo MSSP Alert 2022 (34º no mundo) e líder nos três quadrantes relevantes no ISG Brasil 2022, contratada em licitações recentes por diversos órgãos públicos (CNJ, CJF, CVM, BDMG etc.), com relato do CNJ de estarem prestando bons serviços.
- Future Technologies: No mercado desde 1997, ganhadora da licitação de serviços gerenciados de cibersegurança realizada pelo Poder Judiciário do RJ em outubro 2022, com relato do TJRJ de estarem prestado bons serviços.

- Tripla Service: Fundada em 2015, empresa de referência no mercado local (Belo Horizonte, MG), cujo website apresentava todos os serviços de interesse do TJMG.
- Logicalis: Após contato inicial, não deu prosseguimento nas tratativas.
- Tempest: informou por e-mail que descontinuou a unidade de negócio de venda para governo.
- Deloitte: Não retornou ao contato realizado pelo website.

7.1.2 Contratações similares em outros órgãos

- CNJ. Contrato nº 08/2021 – Contratação de serviços gerenciados de segurança da informação, incluindo serviços de administração, operação e atendimento a requisições, gestão de vulnerabilidades, gestão de incidentes, monitoramento e visibilidade de ataques cibernéticos e testes de invasão. Pagamentos mensais, vigência de **24 meses**.
  - Objeto:
    - Grupo 1: Valor Total **R$ 1.975.751,28**
      - Administração, operação e manutenção e atendimento a requisições [serviço rotineiro mensal]
      - Gestão de vulnerabilidades [serviço rotineiro mensal, 55 aplicações web e 603 servidores físicos e virtuais]
    - Grupo 2: Valor Total **R$ 1.069.479,35**
      - Gestão de incidentes de segurança (CSIRT - Blue Team) [serviço rotineiro mensal]
      - Monitoramento e visibilidade de ataques cibernéticos [serviço rotineiro mensal]
    - Testes de Invasão (Red Team) [serviço sob demanda] Valor Total **R$ 159.799,80**
  - Fornecedor: ISH Tecnologia.
  - O CNJ já possuía soluções de SIEM, NDR, análise de vulnerabilidade de aplicações, EDR, DLP, anti-APT, firewall, proxy, antispam, WAF e balanceador de carga, GRC.
  - Licitou depois:
    - Serviços de apoio à Governança, Riscos e Conformidade – GRC, com fornecimento de software de GRC, incluindo treinamento, manutenção e suporte técnico; e firmou Contrato nº 10/2022 com o fornecedor ISH Tecnologia. Valor Total: **R$ 967.995,00**
    - Serviços e soluções para adequação do CNJ à Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD) e firmou Contrato nº 27/2022 com ISH Tecnologia S.A. **R$ 1.718.000,00**
- TJRJ. Licitação de MSS, Pregão Eletrônico nº 0050/2022, Responsável: Ivan Lindenberg Junior, Assessoria Técnica da Gestão de TIC, Serviços de natureza continuada/rotina, pagamentos mensais, vigência de **24 meses**, valor estimado R$ 50.840.347,44.
  - Fornecedor: Future Technologies Informática Ltda., em 26/08/22, valor **R$ 45.607.999,92**.
  - 13 serviços previstos:
    - Governança e Gestão de Segurança da Informação;
    - Gestão de Risco de Segurança da Informação;
    - Privacidade e Proteção de Dados;
    - Gestão de Segurança de Ativos;
    - Gestão de Incidentes de Segurança, Vulnerabilidades e Ameaças;
    - Gestão de Usuários;
    - Gestão de Problemas;
    - Gestão de Continuidade de Serviços;

- Gestão do Conhecimento;
- Gestão de Comunicação e Educação;
- Gestão de Projetos e Inovações de Segurança da Informação;
- Auditoria e Investigação;
- Melhorias.

- TJRS. Edital de Pregão Eletrônico nº 0005/2022, Contratação de duas empresas distintas especializadas na prestação de serviços gerenciados de segurança da informação.
  - Lote 1: Vencedor: Teletex Computadores e Sistemas Ltda., CNPJ: 79.345.583/0004-95, Valor total: **R$ 11.502.999,84**, vigência **24 meses.**
    - Administração, gerenciamento e monitoração, remotos, dos Serviços de (hardware, software e licenças fornecidos pelo CONTRATANTE):
      - Next Generation Firewall;
      - VPN – Redes Privadas Virtuais;
      - IDS/IPS – Sistemas de Detecção e Prevenção de Intrusão;
      - Firewall de Aplicação (WAF);
      - Anti-SPAM;
      - Proxy/Filtro de Conteúdo Web;
      - Antivírus Corporativo – ambiente de Desktop e Servidores;
    - Implantação, administração, gerenciamento e monitoração, remotos, dos Serviços de (com hardware, software e licenças fornecidos pela CONTRATADA):
      - Gestão de Vulnerabilidades;
      - Filtro de DNS (Domain Name System);
      - PAM (Privileged Access Management).
  - Lote 2: Vencedor: Zerum Research and Technology do Brasil Ltda, CNPJ: 23.870.018/0001-40, Valor total: **R$ 13.959.999,84**, vigência **24 meses**.
    - Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de Network Detection and Response (NDR), com hardware, software e licenças fornecidos, pela CONTRATADA;
    - Administração, gerenciamento e monitoração, remotos, do Serviço de SIEM (Security Information and Event Management), com porte da solução existente, fornecida pelo CONTRATANTE, para nova solução utilizando a stack Elastic Security, com software, licenças e subscrições fornecidas pela CONTRATADA em nome da CONTRATANTE, que será a proprietária da solução;
    - Serviço de Gestão de Incidentes de Segurança para analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado;
    - Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de Testes de Invasão, com hardware, software e licenças fornecidos pela CONTRATADA.
- Superior Tribunal de Justiça (STJ)
  - Pregão Eletrônico nº 027/2023 (ComprasNet), ETP e demais documentos disponíveis no portal de Licitações e Contratos do STJ, abertura da sessão: 27/03/2023. Objeto: Contratação de empresa especializada para prestação de Serviço Gerenciado de Segurança da Informação

(SOC) envolvendo a operação, atendimento e resposta a incidentes com alocação de mão de obra com dedicação exclusiva. Valor estimado: **R$ 13.877.544,50**, vigência **20 meses**.

- Itens do objeto:
  - 1: Serviço de Operação e Atendimento a Requisições e Resposta a Incidentes, com 6 postos de Especialistas em Segurança da Informação e 1 posto de Gerente Técnico;
  - 2: Serviço de Segurança da Informação, 1 unidade global de serviço, incluindo pessoal (mão de obra não exclusiva), softwares e outros recursos, composto por:
    - Serviço de gestão de incidentes de segurança (Blue Team);
    - Serviço de gestão de vulnerabilidades;
    - Serviço de monitoramento e visibilidade de ataques cibernéticos;
    - Serviço de orquestração, automação e resposta de segurança (SOAR);
    - Serviço de gestão antivírus e do serviço de proteção de e-mail.
- Fornecedor 1º colocado: Advanta (Oakmont Group), melhor lance R$ 10.400.000,00, inabilitada em 10/04/2023; 2º colocado: PTLS (Logicalis), valor total **R$ 10.626.125,70** sendo R$ 4.964.027,90 do Item 1 e R$ 5.662.097,80 do Item 2, declarada vencedora em 17/04/2023; 3º: ISH Tecnologia; 4º: Redbelt Security. (Licitação ainda não homologada.)

- O STJ adquiriu à parte a ferramenta de SIEM, como parte do Pregão Eletrônico nº 049/2022, Objeto: Licenças de uso de software Microsoft, adotando a solução em nuvem Microsoft Sentinel, por meio de Créditos Azure (item 2.13 do contrato).
- Pregão Eletrônico nº 043/2021. Objeto: Contratação de empresa especializada em segurança cibernética para prestação de Serviços Gerenciados de Segurança da Informação, em regime de dedicação exclusiva de mão de obra, envolvendo consolidação e visibilidade de eventos de segurança, administração, operação, análises, monitoramento e respostas a incidentes de segurança da informação.

- Conselho da Justiça Federal (CJF)
  - Pregão Eletrônico nº 1/2020, Processo SEI nº 0001989-89.2019.4.90.8000, Edital e anexos.
    - Objeto: Contratação de Serviços Gerenciados de Segurança da Informação para o CJF, com as especificações técnicas contidas no Termo de Referência e Anexos (I a V), compreendendo os seguintes serviços:
      - Serviços de Operação e Atendimento à Requisições;
      - Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team);
      - Serviço de Gestão de Vulnerabilidades;
      - Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos;
      - Serviço de Orquestração, Automação e Resposta de Segurança (SOAR);
      - Serviço de Testes de Invasão (Red Team).
    - Fornecedor: ISH Tecnologia. ARP gerou o Contrato nº 008/2020, vigência **24 meses**, valor total **R$ 2.440.054,88**.
- Comissão de Valores Mobiliários (CVM-RJ)
  - Pregão Eletrônico nº 11/2021, Processo nº 19957.004591/2021-56. Objeto: Contratação de empresas especializadas para a prestação de serviços técnicos na área de Tecnologia da Informação e Comunicações – TIC, compreendendo o fornecimento de Serviços Gerenciados de Segurança da Informação (MSS – Managed Security Services), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

- Itens do objeto:
  - Grupo 1: Contrato nº 18/2021, fornecedor ISH Tecnologia, valor total **R$2.654.640,36**
    - 1: Serviço de Gestão de Vulnerabilidades, **36 meses**
    - 2: Serviços de monitoramento de ataques cibernéticos, 36 meses
    - 3: Serviços de resposta a incidentes de segurança, 36 meses
    - 4: Serviços de operação e resposta a requisições, 36 meses
    - 5: Serviço de conscientização de segurança da informação, 36 meses
  - Grupo 2: Contrato nº 19/2021, fornecedor BeSafe Brasil, valor total **R$ 69.050,40**
    - 6: Serviço de teste de invasão, **6 execuções**.

- Banco do Brasil. Licitação nº 947358 no portal Licitacoes-e, Edital: 2022/02356, Processo: 2022/02356 (7421).
  - Objeto: Registro de preços para aquisição de solução de segurança BAS (Breach and Attack Simulation), com garantia técnica, pelo período de 60 (sessenta) meses.
  - Quantidade: 100 agentes. Fornecedor homologado: Cyber Labs Tecnologia, fabricante Cymulate, valor unitário R$ 45.390,00, valor total **R$ 4.539.000,00**.

7.2 Análise Comparativa de Soluções

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Única	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Única			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Única			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas em padrões de governo ePing, eMag, ePWG?	Única			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Única			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	‘Única			X

7.3 Custos Totais das Soluções - TCO

Propostas preliminares solicitadas a fornecedores de referência:

Solução Única		ISH Tecnologia		10/02/2023	Tripla Service		15/05/2023	Future Tech		13/03/2023
Item	**Unid.**	**Qtd.**	**Unitário R$**	**Total R$**	**Qtd.**	**Unitário R$**	**Total R$**	**Qtd.**	**Unitário R$**	**Total R$**
1. Implantação										
1.1. Levantamento e avaliação inicial da infraestrutura	UN.	1	416.318,47	416.318,47	1	470.492,00	470.492,00	1	110.204,08	110.204,08
1.2. Capacitação	UN.	1	76.100,34	76.100,34	1	207.525,12	207.525,12	1	126.530,61	126.530,61
2. Governança e gestão de segurança										
2.1. Serviços estratégicos de GRC	Mês	36	54.654,05	1.967.545,80	36	217.697,92	7.837.125,12	36	86.326,53	3.107.755,08
2.2. Definição de controles, salvaguardas e remediações	Mês	36	17.363,66	625.091,76	36	217.697,92	7.837.125,12	36	296.938,78	10.689.796,08
3. Monitoramento, detecção e resposta gerenciados										
3.1. Centro (SOC), equipe (ETIR) e gestão de eventos	Mês	36	620.106,91	22.323.848,76	36	956.826,26	34.445.745,36	36	279.591,84	10.065.306,24
3.2. Orquestração, automação e resposta	Mês	36	11.677,30	420.382,80	36	32.512,50	1.170.450,00	36		
3.3. Proteção contra riscos digitais (DRP)	Mês	36	51.136,36	1.840.908,96	36	70.895,31	2.552.231,16	36	197.639,69	7.115.028,84
4. Gestão de vulnerabilidades e testes de segurança										
4.1. Gestão contínua de vulnerabilidades	Mês	36	437.300,53	15.742.819,08	36	329.941,67	11.877.900,12	36	166.784,90	6.004.256,40
4.2. Testes de segurança automatizados (BAS)	Mês	36	29.840,00	1.074.240,00	36	65.025,00	2.340.900,00	36	93.061,22	3.350.203,92
4.3. Testes de invasão (Pentest)	UN.	6	35.820,00	214.920,00	6	63.580,00	381.480,00	6	102.040,82	612.244,92
5. Diagnóstico e avaliação de identidade e acesso	UN.	1	519.337,05	519.337,05	1	86.700,00	86.700,00	1	106.326,53	106.326,53
6. Serviços técnicos especializados, sob demanda	Hora	3600	385,00	1.386.000,00	3600	378,00	1.360.800,00	3600	250,00	900.000,00
TOTAL				**46.607.513,02**			**70.568.474,00**			**42.187.652,70**

Médias:

- Total (36 meses): R$ 53.121.213,24
  - Mensal (serviços continuados): R$ 1.411.006,12 ➔ O valor é compatível com o da licitação do TJRJ, de porte e escopo similar ao TJMG.
  - Anual (incluindo 2 testes de invasão e 1200 horas de serviços técnicos): R$ 17.471.567,28
  - Implantação: R$ 469.056,87
  - Avaliação de identidade e acesso: R$ 237.454,53
  - PenTest (unitário): R$ 67.146,94
  - Hora técnica de serviços especializados (unitário): R$ 337,67.

8 DESCRIÇÃO E JUSTIFICATIVA DA SOLUÇÃO DE TIC A SER CONTRATADA

Contratação de serviços gerenciados de segurança cibernética (*managed security services* - MSS), de natureza continuada, remotos e presenciais, em níveis estratégico, tático e operacional, com fornecimento de equipe técnica especializada, ferramentas, processos e transferência de conhecimento.

O rol de itens e subitens de serviços é conforme a seguir:

Lote 1:

1. Implantação
1.1. Levantamento e avaliação inicial da infraestrutura e dos ativos de TIC
1.2. Capacitação
2. Governança e gestão de segurança de TIC
2.1. Serviços estratégicos de governança, risco e conformidade (GRC)
2.2. Definição de controles, salvaguardas e remediações
3. Monitoramento, detecção e resposta gerenciados de segurança
3.1. Centro de operações de segurança (SOC), equipe de tratamento e resposta a incidentes (ETIR) e gerenciamento e análise de eventos e informações de segurança (SIEM)
3.2. Orquestração e automação e resposta (SOAR)
3.3. Proteção contra riscos digitais (DRP)
4. Gestão de vulnerabilidades e testes de segurança
4.1. Gestão contínua de vulnerabilidades e de exposição a ameaças baseada em riscos
4.2. Testes de segurança automatizados (BAS)
5. Identidade e acesso
5.1. Diagnóstico e avaliação de governança de identidade (IGA) e gestão de acessos (AM)
6. Serviços técnicos especializados, sob demanda

Lote 2:

1. Testes de invasão (PenTest)

Esta composição da solução atende integralmente e está totalmente aderente aos requisitos, bem como se mostrou viável e adequada tanto em consultas ao Gartner quanto em análises de prospecção de mercado por várias empresas e seu rol e segmentação de produtos e serviços ofertados.

9 JUSTIFICAR O PARCELAMENTO OU NÃO DA SOLUÇÃO

A maior parte dos serviços é altamente inter-relacionada entre si. Metodologia, processos e procedimentos definidos pelos serviços estratégicos são seguidos nos serviços de segurança reativos e preventivos, como o tratamento e resposta a incidentes e a gestão de vulnerabilidades e riscos. resultados dos diagnósticos, análises, testes, eventos e incidentes dos serviços reativos e preventivos são o insumo para a definição do plano de controles e salvaguardas de segurança. Os diagnósticos e avaliações realizados na implantação, nos serviços estratégicos e nos serviços de identidade e acesso devem ser complementares e harmônicos entre si.

Os serviços continuados devem tirar proveito da mesma infraestrutura tecnológica e operacional 24 × 7 de alta disponibilidade; e as soluções e ferramentas ofertados devem compor uma arquitetura unificada e harmônica, evitando sobreposições, conflitos e lacunas entre si. Portanto, o não parcelamento destes serviços, além de garantir máxima integração e agilidade na execução dos serviços, reduz significativamente a complexidade técnica e administrativa e pode facilitar uma proposição de serviços e soluções otimizada e favorável à economicidade.

Contudo, o serviço de Testes de Invasão (Pentest), a serem executados de forma esporádica, são testes de segurança nos quais os avaliadores imitam ataques do mundo real, usando as mesmas ferramentas e técnicas usadas por invasores reais, na tentativa de identificar maneiras de contornar os recursos de segurança de aplicativos, sistemas, redes e processos com o objetivo de revelar vulnerabilidades nos sistemas, ativos, controles e processos. Desta forma, eles põem à prova todos os demais serviços e se prestam como um instrumento para simular ataques reais e auditar, na prática, os controles e posturas de segurança cibernética, tal que, pelo princípio de segregação de funções previsto na norma internacional ABNT NBR ISO/IEC 27002:2022 (5.3.a), é indicado o parcelamento deste serviço em lote à parte, executado por fornecedor distinto dos demais serviços.

Além disso, existem empresas especializadas que oferecem o serviço de PenTest, mas não a totalidade dos demais serviços, o que pode contribuir para aumentar a competitividade e especialização no certame. Citamos como exemplo a empresa FreeBSD Brasil[41], que já executou estes serviços anteriormente para o próprio TJMG (Pregão Eletrônico nº 125/2010) com alta qualidade e eficácia.

Modelo similar de divisão em lotes foi adotado pela Comissão de Valores Mobiliários (CVM-RJ) no Pregão Eletrônico nº 11/2021, Processo nº 19957.004591/2021-56.

10 VALIAR NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO PARA VIABILIZAR A EXECUÇÃO CONTRATUAL

10.1 Infraestrutura tecnológica

A maior parte dos serviços é remota, não requerendo infraestrutura tecnológica adicional por parte do Tribunal. Para os serviços e recursos executados em ambiente externo, o Tribunal dispõe da infraestrutura tecnológica suficiente para comportá-los, como pré-disposição no data center e redes de comunicação e acesso à internet.

10.2 Infraestrutura elétrica

Os serviços e recursos internos não devem requerer necessidade adicional de infraestrutura elétrica que demande adequação no ambiente do Tribunal.

10.3 Logística de implantação

Será provido pelo Tribunal o acesso físico às suas dependências aos diretamente envolvidos na prestação dos serviços. Assim como no caso do acesso físico, serão fornecidos o acesso lógico e os

[41] FreeBSD Brasil. Produtos: PenTest, https://www.freebsdbrasil.com.br/produtos/pentest.html, acessado em 31/03/2023.

respectivos privilégios adequados nos sistemas, aplicações, ferramentas e demais ativos necessários à plena execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução, com o devido controle de acesso.

10.4 Espaço físico

O Tribunal deverá disponibilizar sala(s) com o espaço físico necessário e adequado para comportar a equipe de profissionais da empresa alocados internamente, tanto para aqueles em caráter contínuo (equipe dedicada) quanto em caráter eventual em empreitadas ou sob demanda (implantações, avaliações etc.).

10.5 Mobiliário

O Tribunal deverá disponibilizar o mobiliário básico de cadeiras, mesas de escritório e armários necessário para comportar a equipe de profissionais da empresa nos serviços executados internamente.

10.6 Impacto ambiental

Por se tratar de serviços de natureza predominantemente intelectual com uso intensivo de tecnologia da informação, não se vislumbra a priori inadequações ou riscos que representem impacto ambiental, considerando o ambiente físico e tecnológico do Tribunal e as políticas e diretrizes ambientais aplicáveis.

11 NOTAS TÉCNICAS / INFORMAÇÕES ADICIONAIS

O espectro de temas e domínios em segurança cibernética é muito amplo. O objeto da presente contratação foca principalmente a coordenação centralizada de estratégias e ações de governança e gestão de cibersegurança de forma holística para todo o setor de TIC, bem como os aspectos chave de segurança defensiva e ofensiva que se refletem, em maior parte, nas áreas de infraestrutura e operações de TIC.

Diversos temas estão fora do escopo desta contratação e devem ser objeto de iniciativas e projetos em separado, pois envolvem contextos, abrangência e tecnologias específicas. Citamos a seguir alguns destes temas:

- Solução para programa corporativo continuado de educação e conscientização em segurança da informação, segurança cibernética, privacidade e proteção de dados pessoais (*security awarness*), voltadas aos usuários de tecnologia. Contudo, é escopo previsto no Requisito 1.1 de “Requisitos de negócio” ações e campanhas de divulgação e conscientização sob demanda, em geral abordando ameaças preponderantes e normas ou controles implantados.
- O escopo da gestão de vulnerabilidades, para ter maior eficácia e autonomia em efetivamente reduzir a superfície de ataque e a exposição, acaba incluindo parte de capacidades típicos de uma solução de gerenciamento unificado de ativos endpoints

(UEM)[42], incluindo inteligência e automação para descoberta, autoajuste (*self-healing*) e atualizações corretivas (*patching*). Contudo, certas capacidades como distribuição ampla de pacotes (novos e atualizações) e suporte remoto devem requerer iniciativa à parte. Igualmente não é escopo ações para redução do débito técnico, modernização tecnológica e redução de restrições e limitações que reduzam as necessidades de exceções à aplicação de patches, bem como adoção de ferramentas de experiência de usuário interno (DEX)[43] e de testes automatizados de ambientes desktop[44].

- Solução de proteção, detecção e resposta de Endpoints (EPP/EDR)[45] para estações de trabalho e servidores. No escopo da presente contratação, está prevista apenas integração com a atual solução utilizada pelo Tribunal. Contudo, o Tribunal atualmente conta com uma solução razoável de proteção (EPP) que deve ter seu uso otimizado integrado aos novos serviços, enquanto não se concretiza a adoção de nova solução.
- Soluções para governança e administração de identidades (IGA)[46, 47, 48, 49], para gerenciamento de acessos e autorizações (AM)[50] a sistemas, aplicações e serviços de TIC e gerenciamento de acessos privilegiados (PAM). No escopo da presente contratação, contudo, está previsto um levantamento e diagnóstico inicial que subsidiará os estudos técnicos preliminares para contratações subsequentes neste tema.
- Solução para acesso remoto[51] e em nuvem[52, 53], considerando arquiteturas e tecnologias como *zero-trust network access* (ZTNA) e Security Service Edge (SSE)[54].
- Metodologias e tecnologias de desenvolvimento de software seguro e de testes de segurança em aplicações (AST)[55] no desenvolvimento e homologação de softwares, incluindo recursos de análise e testes estáticos, dinâmicos e interativos, análise de componentes de software (SCA) vulneráveis e assistência integrada no ambiente de desenvolvimento (IDE).
- Proteção de dados pessoais, incluindo solução de apoio a gestão e a conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD) e soluções de criptografia e gerenciamento de dados que suportem anonimização e minimização de dados. Contudo, iniciativa de contratação de ferramenta e serviços de apoio a gestão e conformidade à LGPD já está sendo abordada pelo Centro de Governança de Dados e Segurança da Informação Pessoal - CEGINP, em alinhamento com a DIRFOR.

[42] Gartner. Magic Quadrant for Unified Endpoint Management Tools, 01/08/2022, ID G00757534, por Tom Cipolla, Dan Wilson, Chris Silva, Craig Fisler.
[43] Gartner. Market Guide for DEX Tools, 31/08/2022, ID G00764030, por Dan Wilson, Tom Cipolla, Tori Paulman, Autumn Stanish, Stuart Downes.
[44] Gartner. Accelerate Windows and Third-Party Application Patching, 13/02/2023, ID G00784978, por Tom Cipolla, Erin Pierre, Craig Fisler, Sunil Kumar.
[45] Gartner. Magic Quadrant for Endpoint Protection Platforms, 31/12/2022, ID G00752236, por Peter Firstbrook, Chris Silva.
[46] Gartner. Guidance for Identity Governance and Administration, 05/07/2022, ID G00766916, por Homan Farahmand.
[47] Gartner. Solution Criteria for Identity Governance and Administration, 13/12/2019, atualizado em 15/06/2021, ID G00436157, por Paul Mezzera.
[48] Gartner. Solution Comparison for Identity Governance and Administration, 11/11/2022, ID G00771538, por Nat Krishnan, Gautham Mudra.
[49] Gartner. Market Guide for Identity Governance and Administration, 04/07/2022, ID G00741319, por David Collinson, Henrique Teixeira, Kevin Kampman, Rebecca Archambault, Brian Guthrie.
[50] Gartner. Magic Quadrant for Access Management, 01/11/2022, ID G00761397, por Henrique Teixeira, Abhyuday Data, Michael Kelley, James Hoover, Brian Guthrie.
[51] Gartner. Remote Access Options for Enterprise Endpoints, 11/04/2022, ID G00759543, por Thomas Lintemuth.
[52] Gartner. Guide to Cloud Security Concepts, 21/09/2021, ID G00756156, por Patrick Hevesi, Richard Bartley, Dennis Xu.
[53] Gartner. Solution Path for Security in the Public Cloud, 28/01/2022, ID G00757969, por Richard Bartley.
[54] Gartner. Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products, 17/01/2023, ID G00768335, por Dennis Xu, Jon Amato, Patrick Hevesi.
[55] Gartner. Magic Quadrant for Application Security Testing, 18/04/2022, ID G00753626, por Dale Gardner, Mark Horvath, Dionisio Zumerle.

12 RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

12.1 Recursos Materiais

Descrição do Recurso	Quant.	Ação para obtenção do Recurso	Responsável
Espaço físico e mobiliário necessários à equipe presencial nas dependências do TJMG	05	Providenciar espaço físico e mobiliário necessários para alocação da equipe contratada que trabalhará em caráter presencial.	TRIBUNAL
Equipamentos de informática necessários à equipe presencial nas dependências do TJMG	05	Providenciar os equipamentos, incluindo suporte e manutenção/reposição, necessários ao atendimento em seu espaço físico e equipe alocada para trabalhar presencialmente nas dependências do TJMG, consistindo no mínimo de um laptop para cada posto de trabalho presencial, com todos os softwares necessários.	CONTRATADA
Equipamentos para monitoramento nas dependências do TJMG	02	Providenciar os equipamentos, incluindo instalação, suporte e manutenção/reposição, necessários para os painéis de monitoramento (*dashboards*) estratégico-gerencial e tático-operacional, consistindo em dois televisores LED de, no mínimo, 60 polegadas, resolução 4K, em locais a serem indicados dentro das dependências do TJMG na Capital.	CONTRATADA

12.2 Recursos Humanos

A seguir estão as necessidades e quantidades de recursos humanos e as ações necessárias para obtenção deles, com respectivos responsáveis.

Descrição do Recurso	Quant.	Competência	Ação para obtenção do Recurso	Responsável
Gestão estratégica	2	DIRFOR e Presidência	Priorização institucional para garantir liderança e comprometimento da alta gestão, bem como alocação de agenda mensal de acompanhamento.	Diretora Executiva e Juiz Auxiliar da Presidência p/ TIC
Gestores do contrato	3	ATEND/Coord., GETEC e GEOPE	Designação formal no contrato e alocação de agenda semanal para gestão e acompanhamento do contrato.	Assessor e Gerentes das áreas de competência

Fiscais do contrato	3	ATEND/Coord., GETEC e GEOPE	Designação formal, pelo gestor de cada área, de um servidor com dedicação adequada à fiscalização e acompanhamento diário do contrato, seus serviços e atividades.	Assessor e Gerentes das áreas de competência
Equipe de apoio técnico	20	DIRFOR	Designação pelos gestores da DIRFOR dos servidores, além dos gestores e fiscais do contrato, que receberão a capacitação inicial e prestarão apoio técnico necessário à execução dos serviços e suas atividades.	Gestores da DIRFOR

13 ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

A estratégia da continuidade do fornecimento da Solução de TIC em eventual interrupção contratual, em primeiro momento, é bastante limitada, dado o ineditismo da solução. A Diretoria de Informática não possui quadro de servidores especializado e em quantidade suficiente para absorver todos os serviços gerenciados de segurança cibernética pretendidos. Além disso, as tecnologias e ferramentas incorporadas aos serviços são fornecidas como subscrição (software como serviço – SaaS) integrada à prestação dos serviços, o que dificulta sua continuidade em caso de interrupção contratual.

Descrição da ação de continuidade	**Responsáveis**	**Prazos**
Aplicar as cláusulas de penalidade estipuladas para o caso e proceder com nova contratação imediata junto a outro fornecedor, nos mesmos moldes da contratação original.	Gestores e fiscais do contrato; DIRSEP	Na rescisão
A Diretoria de Informática, por meio de seus servidores, terá acompanhamento bem próximo ao processo e à equipe de tratamento e resposta a incidentes de segurança cibernética da contratada, para que possa assumir a responsabilidade por operacionalizar, de forma mínima e emergencial, a continuidade deste processo e da ETIR.	Equipe de apoio técnico	Durante toda a vigência do contrato e execução dos serviços
Identificar, durante a execução dos serviços, determinadas tecnologias e ferramentas que estejam se mostrando altamente essenciais, estratégicas e eficazes à segurança cibernética do Tribunal e considerar a possibilidade de contratá-las diretamente, visando continuidade e independência do provedor de serviços gerenciados de segurança.	Gestores e fiscais do contrato e Equipe de apoio técnico	Durante toda a vigência do contrato e execução dos serviços, em especial no ETP das prorrogações contratuais

14 ESTRATÉGIA DE TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

- Em tempo hábil, deve ser iniciado novo projeto de contratação de forma que um novo contrato se inicie pelo menos 90 dias antes do final da vigência contratual presente, incluindo suas eventuais prorrogações. Os Termos de Referência da presente contratação e da subsequente devem prever os critérios das Fase de Transição Inicial e Transição Final de prestação de serviços, de modo a garantir o pleno repasse de conhecimentos, de dados e de operações de forma ininterrupta, com a gradativa desativação dos serviços que finalizam alinhada com a gradativa ativação dos que os sucedem.
- Ao final do contrato, a CONTRATADA deverá atualizar e/ou elaborar toda a documentação que por acaso não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.
- Ao final do contrato, a CONTRATADA deverá efetuar o repasse de conhecimentos para quem vier a absorver o serviço por meio de reuniões e documentos técnicos e/ou manuais específicos.
- Ao final do contrato, todos as credenciais, perfis e autorizações de acesso da CONTRATADA ao ambiente computacional do Tribunal deverão ser revogadas.
- Ao final do contrato, todas as caixas postais eventualmente criadas para a CONTRATADA deverão ser eliminadas.
- Ao final do contrato, a CONTRATADA deverá realizar a devolução de todos os recursos materiais eventualmente disponibilizados pelo TJMG.

15 ESTRATÉGIA DE INDEPENDÊNCIA

- Elaborar e apresentar pareceres técnicos de análise, esclarecimento, orientação e recomendações sobre demandas e assuntos especializados relacionados, seja proativamente, quando identificada necessidade pela contratada, ou sob demanda, mediante a formalização da solicitação pelo Tribunal, relacionados a quaisquer dos serviços prestados.
- Todos os logs consolidados e repositórios de dados e análises no SIEM para consulta “a quente” dos últimos 12 meses, no mínimo, mais a integralidade das regras, casos de uso e *playbooks*, bem como do histórico de registro eventos e incidentes de segurança, devem estar continuamente disponíveis ao Tribunal. Todas essas informações devem ser exportadas e fornecidas em formato completo, aberto e interoperável ao final do contrato.
- A CONTRATADA cederá ao TRIBUNAL, nos termos do artigo 111 da Lei nº 8.666/93, o direito patrimonial e a propriedade intelectual, em caráter definitivo, de todos e quaisquer produtos e resultados gerados em consequência do cumprimento deste contrato, podendo o TRIBUNAL proceder às modificações necessárias à continuidade do serviço e/ou contratar terceiros para fazê-lo.
    - Entendem-se por resultados relatórios, análises, estudos e pareceres técnicos; normativos e planos; documentação; casos de uso; *playbooks* e *runbooks*; controles e salvaguardas propostos e implantados; scripts; códigos fonte; protótipos; registros, modelos e bases de dados; e qualquer outro conteúdo ou informação produzido exclusivamente em decorrência da execução dos serviços.

- A CONTRATADA cederá também ao TRIBUNAL os direitos autorais vinculados à prestação dos serviços, nos termos do artigo 4º da Lei nº 9.609/1998, referentes a todos e quaisquer produtos e resultados gerados em consequência do cumprimento deste contrato.
    - Caberá à CONTRATADA arcar com quaisquer valores decorrentes de imputação judicial ao TRIBUNAL, relativos a esses direitos.
- Ficam resguardados os direitos autorais de resultados ou produtos decorrentes da execução dos serviços que tenham prévia restrição de direitos de propriedade patrimonial e intelectual ou autorais da CONTRATADA ou de terceiros, devendo nestes casos ser concedido o direito de uso mais amplo possível ao TRIBUNAL, visando sua continuidade e independência.

16 APROVAÇÃO E ASSINATURA

Integrante Técnico	**Integrante Demandante**
Paulo Henrique Morais Machado Analista de Sistemas – ATEND 006979-9	Márcio Henrique C. d'Ávila Coordenador de Cibersegurança – ATEND 002292-1
A ATEND realizou a análise de conformidade do documento de acordo com Resolução nº 468/2022 do Conselho Nacional de Justiça.	
Paulo Viallet Neto Analista de Sistemas – ATEND 008522-5	Mateus Cançado Assis Assessor Técnico – ATEND 006375-0

Autoridade Máxima da Área de TIC (ou Autoridade Superior, se aplicável)
Alessandra da Silva Campos Diretora Executiva de Informática – DIRFOR 007580-4