

ANEXO I**TERMO DE REFERÊNCIA – ESPECIFICAÇÃO TÉCNICA****OBJETO**

Contratação de empresa para fornecimento de Serviço de gerenciamento e correlacionamento de eventos e informações de segurança SIEM (Security Information and Event Management) e SOAR (Serviço de Orquestração, Automação e Resposta de Segurança) baseada em nuvem (SaaS), com garantia e suporte 24x7, incluindo Serviços de Suporte à Solução que compreendem a implantação, atualização tecnológica, suporte técnico, administração e operação da infraestrutura e os serviços especializados de prospecção, construção, customização e integração de casos de uso, scripts e interpretadores (parsers) e transferência de conhecimento, pelo prazo de 36 (trinta e seis) meses.

REQUISITOS GERAIS DA SOLUÇÃO

1. Licenciamento das ferramentas SIEM e SOAR: Fornecimento de licenças para a plataforma SIEM e SOAR, ambas desenvolvidas pelo mesmo fabricante.
2. Atualização Tecnológica: Para qualquer módulo da solução, a CONTRATADA deverá garantir a atualização de todos os itens novos inseridos na solução, durante todo o período contratado sem qualquer cobrança adicional por funcionalidades ou melhorias existentes, garantindo sempre que a CAIXA possua a versão mais atualizada possível da solução.
3. A solução deve ser capaz de ler, interpretar, padronizar e correlacionar eventos provenientes de registros de diferentes fontes com a finalidade de detectar eventos de segurança e vulnerabilidades.
4. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, com pelo menos uma cópia atualizada de segurança também no Brasil.
5. Ser estruturada como um item integral e exclusivo voltado a suprir as necessidades de monitoramento, segurança, análise, investigação e proteção cibernética.
6. Ser composta pelas seguintes funcionalidades ou equivalentes:
 - 6.1.1. Console de administração, operação, monitoramento e pesquisa da solução;
 - 6.1.2. Coletores de eventos (LOG/FLOW);
 - 6.1.3. Correlacionador de eventos;
 - 6.1.4. Armazenador de eventos e registros processados;
 - 6.1.5. Análise de comportamento de usuário e dispositivos (UEBA);
 - 6.1.6. Orquestração, automação e resposta de incidentes de segurança (SOAR).
7. Deve possuir conformidade com as normas ISO 27001 e LGPD/GDPR

8. Deve possuir biblioteca de casos de uso do fabricante, que contenha conteúdo para download que inclua pacotes especializados de dashboards e coletores desenvolvidos pelo fabricante.
- 8.1. Deve possuir casos de uso disponíveis para as seguintes tecnologias em uso na infraestrutura tecnológica da CAIXA:
 - 8.1.1. Azure Active Directory Identity Protection.
 - 8.1.2. Microsoft Defender for Identity.
 - 8.1.3. Microsoft Defender for Office 365.
 - 8.1.4. Microsoft Defender for Cloud.
 - 8.1.5. Microsoft Defender for Cloud Apps.
 - 8.1.6. Prevenção Contra Perda de Dados - DLP; (MIP – Microsoft Information Protection e Microsoft Purview)
 - 8.1.7. Microsoft Intune.
 - 8.1.8. Microsoft Defender for Endpoint.
 - 8.1.9. Azure Firewall.
 - 8.1.10. Azure Key Vault.
 - 8.1.11. Microsoft 365 Insider Risk Management.
 - 8.1.12. Threat Intelligence Platforms.
9. Deve garantir disponibilidade de 99,9%.
10. O acesso padrão para conexão com a Rede Caixa (conexão entre a CONTRATADA e a CAIXA) deverá ser realizado mediante o uso de circuito privado dedicado nas tecnologias LAN-to-LAN ou MPLS e fornecido pela CONTRATADA, conforme descrito no ANEXO I-F – CONEXÃO CAIXA.
11. A Solução deverá estar disponível para funcionamento ininterrupto (24X7).
12. Deve possuir suporte técnico para todos os itens da solução em língua portuguesa ou inglês.
13. Deve possibilitar o desenvolvimento de scripts para integrar os alertas gerados na solução de SIEM com a solução de gerenciamento de incidentes cibernéticos em uso atualmente na CAIXA (The Hive Project – Version 4.1).
14. Inteligência Artificial (IA) para aprimorar a detecção, análise e resposta a ameaças.
 - 14.1. Deve integrar IA para Detecção Aprimorada de Ameaças:
 - 14.1.1. Empregar algoritmos de aprendizado de máquina para identificar padrões anormais e atividades suspeitas em logs e eventos de segurança em tempo real.
 - 14.1.2. Capacitar o sistema para detectar ameaças emergentes e desconhecidas, adaptando-se às características do ambiente de TI da CAIXA.
 - 14.1.3. Permitir a personalização da detecção de anomalias, ajustando a sensibilidade de acordo com os requisitos específicos.
 - 14.1.4. Listar incidentes baseados em datas, severidade ou através de algum metadado informado (IP, Hash, Conta de usuário etc.)
 - 14.1.5. Retornar informações para o enriquecimento de incidentes acionando serviços de Threat Intelligence
 - 14.1.6. Gerar sugestões de regras de automação de acordo com incidentes gerados na plataforma

- 14.1.7. Gerar sugestões de melhorias baseando-se em pesquisas realizadas por usuários com base no uso de linguagens de manipulação de dados utilizadas na criação de queries para investigação ou hunting.
- 14.2. Deve implementar IA para Análise Avançada de Ameaças:
 - 14.2.1. Integrar técnicas de processamento de linguagem natural (PLN) para extrair informações relevantes de logs, relatórios de incidentes e outras fontes de dados.
 - 14.2.2. Correlacionar eventos de diferentes fontes para mapear cenários de ataque, determinar o escopo do comprometimento e identificar a raiz das causas.
 - 14.2.3. Facilitar a visualização gráfica dos eventos correlacionados para auxiliar na compreensão da linha do tempo do ataque e das interações entre os componentes da infraestrutura.
- 14.3. Deve implementar IA para Priorização Inteligente de Alertas:
 - 14.3.1. Implementar um sistema de pontuação de risco baseado em IA para priorizar alertas de segurança, considerando fatores como severidade da ameaça, histórico de ataques e potencial impacto no negócio.
 - 14.3.2. Permitir a personalização da pontuação de risco de acordo com as necessidades da CAIXA, ajustando a importância de cada fator.
 - 14.3.3. Notificar os analistas de segurança sobre alertas críticos em tempo real, facilitando a resposta imediata a incidentes graves.
- 14.4. Deve implementar IA para Investigação Automatizada:
 - 14.4.1. Automatizar tarefas repetitivas de investigação, como coleta de informações sobre ameaças conhecidas, busca por indicadores de comprometimento (IoCs) em logs e eventos de segurança e análise de arquivos suspeitos.
 - 14.4.2. Gerar insights sobre as investigações, incluindo detalhes sobre a natureza da ameaça, o escopo do comprometimento e recomendar ações a serem tomadas.
- 14.5. Deve implementar IA para Respostas Personalizadas a Incidentes:
 - 14.5.1. Auxiliar na definição de planos de resposta a incidentes personalizados, com base na natureza da ameaça, no contexto do ataque e nas características do ambiente de TI da CAIXA.
 - 14.5.2. Recomendar medidas de mitigação adequadas para conter o incidente, minimizar o impacto nos negócios e prevenir recorrências.
 - 14.5.3. Deve ser capaz de lidar com grandes volumes de dados de segurança e eventos em tempo real, adaptando-se ao crescimento da infraestrutura da CAIXA.
- 15. Deve permitir Automações para Triagem, Notificação, Enriquecimento, Sincronismo e Resposta automatizada.
- 16. A solução deve possuir conectores desenvolvidos e suportados pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos os coletores nativos com informações detalhadas de configurações de cada ativo suportado.
- 17. Os coletores da solução devem ser capazes de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real (near-real-time).

18. A solução deve possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução.

REQUISITOS TÉCNICOS DA SOLUÇÃO

19. A solução deve coletar, aplicar parsing, normalizar, classificar, agregar informações, sumarizar, processar regras e armazenar os dados recebidos em tempo real.
20. Ser capaz de demonstrar perfil de tráfego normalizado em tempo real e traçar o comportamento padrão (baseline) dos ativos e fornecer alertas quando ocorrer eventos fora do baseline;
21. Correlacionar os eventos coletados objetivando evidenciar incidentes que possam ser caracterizados como ataque;
22. A correlação e o armazenamento dos logs e eventos devem ser realizados em processos paralelo;
23. Implementar regras avançadas que ligam eventos sem correlação direta e gerar incidentes caso seja constatado algum desvio;
24. Ser capaz de realizar contextualização, utilizando dados de diferentes origens (rede, servidor, aplicações) em uma única console, otimizando e auxiliando o processo de análise de resposta a incidentes;
25. Implementar a normalização e categorização de logs e flows de rede;
26. Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada. Os eventos e flows devem ser sempre armazenados de forma comprimida;
27. A comunicação entre os componentes da solução deve ser efetuada de forma segura e com criptografia;
28. Funcionar em IPv4 e IPv6;
29. Possuir a capacidade de tratar eventos em formato compactado sem a necessidade de descompressão manual;
30. Realizar o filtro e a seleção dos eventos que deverão ser tratados pela equipe responsável pela segurança tecnológica frente aos incidentes detectados.
31. Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes:
- 31.1. SYSLOG, SYSLOG-NG, SYSLOG com TLS, SNMP (V1, V2 e V3), Microsoft Windows Event Logging API, Microsoft Windows RPC, LOG SMF, FTP, SCP, SFTP, arquivos de logs em texto formatado (vírgula/tabulação/delimitado) e logs em texto não formatado, JDBC e ODBC.
- 31.2. Utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria no mínimo SHA2 e HMAC;
- 31.3. Ter capacidade de capturar, normalizar e realizar o tratamento de eventos em tempo próximo ao real;
- 31.4. Ser capaz de exportar os eventos normalizados no mínimo em CEF (Common Event Format), LEEF (Log Event Extended Format), Syslog (RFC5424) ou CSV;
- 31.5. Fazer a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo ou quantidade de eventos específicos.

32. A solução deve possibilitar a ofuscação de campos sensíveis dos eventos (como senhas, identidade funcional, números de cartões de crédito e outros similares).
33. A solução deve ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listados abaixo:
- 33.1. Firewalls: CISCO, Checkpoint;
- 33.2. Switches: CISCO e Huawei;
- 33.3. Balanceadores de carga: F5, A10, Citrix;
- 33.4. Plataformas de Virtualização: VMware ESX, HyperV e Oracle VM;
- 33.5. Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOS, Oracle Linux), Windows Server (2008, 2012, 2016) e FreeBSD;
- 33.6. Antivírus: McAfee, Microsoft Defender;
- 33.7. Servidores de E-mail: Microsoft Exchange, Office365;
- 33.7.1. Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e Microsoft IIS7 (ou superior);
- 33.8. VPN: Cisco VPN e OpenVPN;
- 33.9. Essa lista é dinâmica e irá evoluir à medida que outros ativos forem demandados para a CONTRATADA.
34. Deve ser capaz de identificar e normalizar, no mínimo, os eventos dos logs dos sistemas e ativos listados:
- Active Directory
 - Apache
 - Cisco ISE
 - Cisco SourceFire Defense Center
 - ClearPass
 - LDAP
 - McAfee Endpoint Protection – Advanced Suite
 - McAfee ePolicy Orchestrator
 - Microsoft DHCP
 - Microsoft TMG
 - Mainframe
 - RRAS Server
 - OpenLDAP
 - Postfix
 - VDI (VMWare Horizon)
 - DNS
 - Guardium
 - Office 365
 - Microsoft Exchange
- 34.1. Essa lista é dinâmica e irá evoluir à medida que outros casos de usos forem demandados para a CONTRATADA.

35. Deve ser capaz de coletar logs de Mainframe z/OS de forma nativa ou com uso de agente externo (RACF, ACF2, Top Secret, DB2, CICS, dentre outros)
36. Os demais logs dos sistemas e ativos que não sejam nativamente suportados deverão ser customizados na ferramenta durante a implantação, bem como durante o período contratado para suporte pelo proponente.

CAPACIDADE

Ingestão de Logs	Retenção Quente (Processamento)	Retenção Longo Prazo (Consultas)
3200 GB/dia	3 meses	33 meses
Retenção Total: 36 meses		

Tabela 1 - Ingestão e Retenção

37. Para a capacidade citada no item acima, deve-se considerar a utilização atual de logs ingeridos e que deverão ser migrados para a nova ferramenta de SIEM, conforme detalhamento abaixo para 2000 GB/dia.

2000 GB/DIA UTILIZADOS ATUALMENTE	
TECNOLOGIAS	PERCENTUAL % DE INGESTÃO
Microsoft Defender for Endpoint	46,50
Active Directory	21,41
Cisco ASA	8,82
Oracle SunOne Directory Server	6,60
Azure - Syslog	4,31
Microsoft Defender for Cloud Apps	3,83
Mainframe z/OS events	2,07
Single Sign-On	1,51
McAfee Web Gateway	1,16
Microsoft Defender for Office 365	1,01
OpenLDAP	1,01
Microsoft Defender for Identity	0,60
Azure Active Directory	0,43
Azure Firewall e outros	0,25
Microsoft Forefront TMG	0,25
Cisco ISE	0,15
Microsoft DHCP Server Log	0,05
Bind DNS	0,05
TOTAL	100,00

Tabela 2 – Distribuição de logs ingeridos atualmente

- 38. Espera-se, no decorrer do contrato, um crescimento na ingestão de logs no SIEM de aproximadamente 1200 GB/dia totalizando, portanto, 3200 GB/dia na capacidade total contratada.
- 39. Deve ser capaz de INGERIR, processar, correlacionar e *armazenar* no mínimo 3200 GB/dia, sem perda de desempenho. Caso a solução ofertada seja contabilizada de outra forma, considerar o tamanho médio de bytes por EPS de 512 bytes;
- 40. Ter capacidade de provisionar recursos para tratar rajadas de no mínimo 100% do consumo diário (auto scaling) sem perda de desempenho.
- 41. Caso ocorra excesso de eventos que ultrapasse o limite contratado, não poderá ocorrer o descarte ou não aproveitamento dos logs;
- 42. **A CAIXA somente irá utilizar aquilo que se propõe a pagar no contrato, ou seja, não haverá pagamento excedente e, por este motivo, não é esperado que a ferramenta processe mais do que esteja sendo previsto, exceto por variações de ingestão comuns a qualquer ferramenta de SIEM.**

CORRELACIONAMENTO

- 43. O Correlacionador deve ser capaz no mínimo de:
- 44. Inserir os alertas e incidentes gerados no próprio fluxo de correlacionamento ou no fluxo de eventos, possibilitando a detecção de padrões mais complexos de ameaças ou violações de conformidade;
- 45. Identificar anomalias baseada em eventos e dados temporais por período determinado pelo operador;
- 46. Realizar o correlacionamento de eventos e alertas utilizando lista de observação (watchlist);
- 47. Permitir a criação e alteração de lista de observação (watchlist);
- 48. Priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:
 - 48.1. Severidade do evento;
 - 48.2. Criticidade do ativo;
 - 48.3. Existência de vulnerabilidade no ativo.
- 49. Possuir capacidade de correlacionar eventos de diferentes ativos do mesmo tipo e de ativos de diferentes tipos;
- 50. Possuir nativamente no mínimo 300 regras de correlacionamento;
- 51. As regras de correlacionamento devem ser passíveis de customização;
- 52. Permitir clonar as regras e renomear as mesmas para posterior alteração;
- 53. Possibilitar a criação de encadeamento de correlacionamentos. Uma ou mais regra de correlacionamento pode ser utilizado dentro de outra regra;
- 54. Tolerar atributos dinâmicos na construção de regras de correlacionamento.
 - 54.1. Entende-se como dinâmicos objetos que sofrem alteração a cada iteração;
- 55. Permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos e tráfego, quando comparados a outros períodos similares;
- 56. Permitir o consumo de base de dados externas, através de feeds para a correlação com eventos coletados pela solução, gerando alertas para cada match em regra de correlacionamento nativa ou customizada.

Análise de comportamento de usuário e dispositivos

Tipo	Quantidade
Endpoints	120.000
Usuários	140.000

Tabela 3 - Quantidade de ativos UEBA

- 57. Implementar ferramenta de análise comportamental de dispositivo e usuários;
- 58. Utilizar algoritmos de Inteligência Artificial para categorizar e analisar o comportamento das entidades. Entende-se como algoritmos de inteligência artificial no mínimo:
 - 58.1. **Implementar algoritmos de Inteligência Artificial, incluindo técnicas de aprendizado supervisionado e não supervisionado.**
- 59. Implementar geração de score de risco baseado em atributos das entidades e eventos coletados pela solução;
- 60. A solução deve ser capaz de realizar consultas de forma online em bases de usuários LDAP e Microsoft Active Directory para detectar potenciais ameaças para a criação de regras de correlação utilizando tais informações coletadas;
- 61. As importações deverão ser nativas ou de forma customizada via API. No caso de construção de customização o desenvolvimento e suporte devem ser efetuadas pelo proponente sem ônus para a CAIXA;
- 62. Permitir criação de lista de observação de entidades para monitoração e rastreamento;
- 63. Permitir criação de lista de não observação de entidades, ou seja, lista de exclusão, para computação de score e outros eventos;
- 64. Possuir dashboard dos usuários com risco alto e realizar drill down para detalhar o score;
- 65. Detectar anomalias no comportamento usual de determinado ente (dispositivo e usuário) e no mínimo detectar desvios:
 - 65.1. Relacionado ao tempo ou ações em tempos inexecutáveis;
 - 65.2. Relacionado a volumetria de dados;
 - 65.3. As fontes e destino dos eventos;
 - 65.4. Localização geográfica;
 - 65.5. Direcionamento e serviços de origem e destino;
 - 65.6. Usuário executando comandos em blacklist;
 - 65.7. Acesso a endereços considerados suspeitos via Threat Feed e IP reputation;
 - 65.8. Contas utilizadas de forma não compatível;
 - 65.9. Uso não compatível de contas de serviço;
 - 65.10. Acessos em arquivos sensíveis dos sistemas.
- 66. Ter conjunto de regras default para casos de uso de UEBA;
- 67. As regras padrões do UEBA devem ser passíveis de customização;
- 68. Ter funcionalidade de aprendizado de comportamento padrão dos entes de forma automatizada.
 - 68.1. O aprendizado deve ser passível de customização pelo operador da solução;

- 69. Ter capacidade de analisar comportamento baseado em aprendizado das ações de usuários de forma automática e ser capaz de detectar desvios de padrões através de regras automáticas;
- 69.1. Implementar algoritmos de Inteligência Artificial, incluindo técnicas de aprendizado supervisionado e não supervisionado.
- 69.2. Aprendizado de máquina e análise de comportamento: Utilização de técnicas de aprendizado de máquina para detecção de anomalias e identificação de ameaças com base no comportamento.

FUNÇÃO ORQUESTRAÇÃO - SOAR (SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE) PARA APRIMORAR A CAPACIDADE DE RESPOSTA A AMEAÇAS DE SEGURANÇA E OTIMIZAR A OPERAÇÃO DO SIEM

- 70. As funções mínimas que a solução deve possuir incluem:
- 70.1. Orquestração de tarefas: Capacidade de automatizar ações de resposta a incidentes, como bloquear endereços IP, desativar contas de usuário ou isolar dispositivos comprometidos.
- 70.1.1. Gerar playbooks listando ações de tarefas para ataques conhecidos ou ocorridos na plataforma
- 70.2. Integração com fontes de dados: Conexão com várias fontes de dados, como logs de segurança, feeds de ameaças, ferramentas de análise de vulnerabilidades, para obter informações relevantes e contextuais.
- 70.3. Correlação de eventos: Análise de eventos e alertas de segurança para identificar incidentes significativos por meio de regras personalizadas ou IA.
- 70.4. Gestão de casos e incidentes: Registro e acompanhamento de incidentes de segurança, permitindo que as equipes de resposta colaborem e documentem suas atividades.
- 70.5. Automatização de fluxos de trabalho: Criação de fluxos de trabalho de resposta automatizada que podem acionar ações específicas com base em regras ou cenários de ameaça.
- 70.6. Enriquecimento de informações: Enriquecimento de dados de eventos com informações contextuais, como dados de ameaças conhecidas, informações sobre ativos e usuários.
- 70.7. Geração de relatórios e dashboards: Criação de relatórios personalizados e painéis de controle para monitorar o desempenho e a eficácia das atividades de segurança.
- 70.8. Notificação e alertas: Capacidade de gerar alertas e notificações em tempo real para as equipes de segurança em caso de incidentes críticos.
- 70.9. Extensibilidade: Possibilidade de adicionar novas integrações, criar scripts personalizados e personalizar as regras e a lógica de automação.
- 70.10. Gestão de políticas: Definição e implementação de políticas de segurança e conformidade por meio de automação.

INTELIGÊNCIA DE AMEAÇAS E SCANNER DE VULNERABILIDADE

- 71. Possuir integração com rede de inteligência (threat intelligence) para atualização constante de feeds de ameaças.
- 72. A nuvem de inteligência deve ter a capacidade de no mínimo consultas de reputação de IP, Georreferência, DNS, HASH e Nome de processos;
- 73. Os dados de georreferenciamento devem ser fornecidos pela solução de forma nativa;
- 74. Implementar coleta de dados de feeds externos para enriquecimento das análises;
- 75. Ser capaz de inserir nos eventos normalizados metadados sobre georreferência;
- 76. Ter capacidade de obter informações de georreferência e imputar essa informação nas correlações e pesquisas;
- 77. Implementar importação de STIX/TAXII e OpenIOC;
- 78. Utilizar informações obtidas por scanner de vulnerabilidade para geração de alertas na solução.

REQUISITOS TÉCNICOS DA CONSOLE DE GERENCIAMENTO

- 79. Requisitos operacionais
 - 79.1. Para garantir a precisão e a consistência dos registros de eventos, o sistema deve incluir:
 - 79.1.1. Conexão com servidor NTP (Network Time Protocol): Garantir a sincronização precisa do relógio do sistema com um servidor de tempo confiável. É crucial que a conexão NTP seja configurada de forma a respeitar e preservar os fusos horários originais dos eventos registrados nos ativos da infraestrutura tecnológica da CAIXA, para evitar discrepâncias e garantir a integridade dos dados de tempo em todos os registros.
 - 79.2. Ser capaz de exportar configurações e regras do centralizador na forma de backup em arquivo e para servidor ftp, sftp e scp;
 - 79.3. Possuir funcionalidade de gerenciamento e configuração centralizados das partes distribuídas da solução;
 - 79.4. As funções de manutenção, operação, pesquisa e administração da solução devem estar integradas na mesma console;
 - 79.5. Implementar a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica.
 - 79.6. A solução deve utilizar recursos como Node-Links para demonstrar ataques correlacionados de forma gráfica, facilitando a visualização do panorama de ameaças e a compreensão do fluxo de ataques.
- 80. Consultas e pesquisa
 - 80.1. Ter funcionalidade de consulta no mínimo das seguintes informações:
 - 80.1.1. Data Início e Fim;
 - 80.1.2. Hash;
 - 80.1.3. Nome do processo;
 - 80.1.4. Nome da Máquina;
 - 80.1.5. IP;

- 80.1.6. Tipo de ataque/detecção;
- 80.1.7. Nome do Evento;
- 80.1.8. Categoria do Evento.
- 80.2. Possibilitar exibição das consultas em gráfico ou tabelas;
- 80.3. Permitir o uso de operadores lógicos, hashes, string ou frases;
- 80.4. No campo de pesquisa deve permitir a construção de consulta em sintaxe similar a SQL com os operadores de consulta;
- 80.5. Permitir a pesquisa nos eventos históricos, fornecendo capacidade de drill down, ou seja, visualizar os detalhes dos eventos, inclusive dados “raw”, quando aplicável, para análise forense e investigação de incidentes.
- 81. Alertas
- 81.1. Mostrar a informação sobre os eventos que compõem um alerta ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente;
- 81.2. Ter um sistema de alertas personalizável pelo administrador que poderá configurar o motivo do disparo do alerta, como ataques identificados;
- 81.3. Ser capaz de enviar alertas e dados nativamente com opção de selecionar quais alertas serão enviados, via protocolo syslog, e de forma automatizada;
- 81.4. A console do Gerenciador deverá ter a funcionalidade de apresentar automaticamente alertas pré-configurados em tempo real;
- 81.5. Prover triagem dos alertas, auxiliando na priorização, investigação e evidenciar o estado dos alertas gerados pela ferramenta;
- 81.6. Fornecer a funcionalidade de geração de alertas (sonoros ou visuais) via dashboard e e-mail para incidentes de alta criticidade detectados no correlacionamento de eventos;
- 81.7. Prover notificação de administrador ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.

RELATÓRIOS

- 82. Gerar relatórios a partir dos dados monitorados;
- 83. Gerar relatórios automatizados configuráveis em períodos, por hora, por dia, por semana, por mês e por ano com envio automático de e-mail, configuráveis pelo administrador;
- 84. Ser gerados em diversos formatos como: texto ou CSV, PDF e XLS;
- 85. Conter, no mínimo:
 - 85.1. Informações por usuário ou dispositivo;
 - 85.2. Informações de ataques identificados;
 - 85.3. Informações de ataques bloqueados;
 - 85.4. Informações de logs sources que não enviam eventos;
 - 85.5. Informações baseado em eventos (watchlist).

DASHBOARD

- 86. Apresentar painéis de controles gráficos (dashboards) que mostrem o status do ambiente, dos logs de eventos, comportamento dos usuários, comportamento

- de outras entidades (entity), incidentes e alertas gerados, fluxos de rede, ameaças e vulnerabilidades, além de permitir a customização com consultas ad-hoc, quando se fizerem necessárias;
- 87. Demonstrar ameaças de alta severidade para o ambiente;
 - 88. Demonstrar os principais meios e tipos de ataques;
 - 89. Identificar automaticamente e mostrar em destaque incidentes de alta prioridade.
 - 90. Possuir capacidade de mapeamento de campos de forma manual e customizada de qualquer tipo de logs;
 - 91. Após o mapeamento do campo, a solução deve ser capaz de efetuar correlacionamentos dos logs previamente existentes, extrair as informações necessárias e fazer os correlacionamentos existentes;
 - 92. O mecanismo de extração e mapeamento dos campos deve possuir no mínimo uso de regex, json ou funcionalidade inerente e nativa da solução;
 - 93. Ter interface GUI para mapeamento dos campos;
 - 94. Ter capacidade de identificação dos tipos de campos conhecidos, durante a normalização, de forma automática de no mínimo: data, hora, ip, porta, usuário, nome do evento e serviço;
 - 95. Permitir a coleta ativa de logs em servidores tftp, ftp e ssh com autenticação via credencial e certificado digital.
 - 96. Permitir iteração básica de textos nas ameaças/eventos alarmados. Cada iteração anotada deve registrar no mínimo a data e o usuário que fez a anotação.
 - 97. Remontagem de ataque (timeline)
 - 97.1. Mapear, correlacionar e demonstrar na forma visual e em “linha do tempo” o incidente resultante de regra de correlação;
 - 97.2. Mostrar as fases do ataque e as informações como hora, ip, usuário, nome do arquivo e link acessado.

ADMINISTRAÇÃO E AUTENTICAÇÃO DE USUÁRIOS E CONTROLE DE ACESSO

- 98. O Gerenciador deverá ser remotamente administrável por meio de interface gráfica (GUI), utilizando canais autenticados e criptografados;
- 99. Os acessos administrativos devem ser autenticados, criptografados e com registros mantidos;
- 100. Autenticar e autorizar usuários administrativos por meio dos protocolos LDAPS, AD, SAML ou OAuth2.0;
- 101. Ser capaz de segregar perfis de acesso, permitindo diferentes níveis de acesso à console de gerenciamento, onde cada perfil possa ter permissões específicas associadas à sua função. No mínimo:
 - 101.1. Admin;
 - 101.2. Operador;
 - 101.3. Leitura.
- 102. As atribuições de acesso e autorização devem permitir customização de diferentes visualizações/dashboard de informações e log sources;

103. Permitir que os perfis de acesso sejam relacionados a grupo de usuários para possibilitar, conceder ou revogar acessos conforme a inclusão ou exclusão de usuários desses grupos;
104. Permitir múltiplos acessos simultâneos à console de gerenciamento, seja para análise de informações ou aplicação de configurações.
105. Deve oferecer um mecanismo de segundo fator de autenticação para acesso ao console de gerenciamento, garantindo um nível adicional de segurança.

SERVIÇOS DE SUPORTE À SOLUÇÃO

106. Os serviços de suporte à solução compreendem a implantação, sustentação, atualização tecnológica durante todo o contrato, suporte técnico, administração e operação da infraestrutura tecnológica.
107. Entende-se por serviços de suporte técnico a prestação de serviços visando à reparação de eventuais falhas ou inconsistências detectadas nos serviços (quer sejam produtos de hardware e/ou software), de forma a garantir o pleno, correto e seguro funcionamento dos serviços e seus módulos ou componentes e suas integrações com o ambiente CAIXA, assim como na prestação de informações necessárias ao esclarecimento de dúvidas sobre o funcionamento dos serviços e dos seus módulos e/ou componentes, promovendo sua perfeita operacionalização.
108. O Suporte Técnico consiste na atuação de caráter predominantemente reativo, com acionamento sob demanda, envolvendo o tratamento de falhas, interrupções ou redução de desempenho no uso dos serviços por parte da CAIXA, mas envolve também atuação proativa na medida em que trata situações de falhas que não cheguem a afetar a qualidade e/ou desempenho dos serviços consumidos pela CAIXA.
109. Compreendem ainda os serviços especializados de prospecção, construção, customização e integração de casos de uso, API, scripts e interpretadores (parsers), abrangem todas as atividades de pesquisa no mercado, portais e comunidades de cibersegurança, mediante solicitação da CAIXA ou por identificação da CONTRATADA de forma proativa, de casos de uso e soluções adequadas às necessidades constatadas ou suscitadas, bem como a realização de customizações para que estes atendam às regras de negócios, a integração a outros sistemas em produção e aos padrões de segurança tecnológica da CAIXA, compreendendo as seguintes tarefas básicas:
 - Desenvolvimento de parsers necessários para construção de casos de usos definidos pela CAIXA;
 - Desenvolvimento de scripts;
 - Aperfeiçoamento e customizações de soluções e serviços;
 - Planejamento de soluções e serviços;
 - Mentoring;
 - Adaptação evolutiva e customizações;
 - Implementação de novos casos de usos definidos pela CAIXA;

- Definição e construção de integrações entre as soluções/tecnologias do produto com as demais soluções/ferramentas utilizadas pela CAIXA;
 - Criação e customização de relatórios personalizados.
110. As melhorias ou customizações solicitadas pela CAIXA deverão ser consultadas pela CONTRATADA junto ao fabricante e/ou comunidade oficial do produto para verificar a existência de esforços em curso para o assunto em questão.
111. Os serviços especializados serão solicitados, sob demanda e a critério da CAIXA, sendo validados conforme SLA acordado.
112. A construção de casos de uso, parsers, scripts, e demais componentes poderá, a critério da CAIXA, ser executado fora das instalações da CONTRATANTE de forma remota com acompanhamento e ponto de controle diário.
113. Todos os processos de customização de componentes, mesmo aqueles decorrentes da iniciativa da CONTRATADA, deverão ser previamente autorizados pela CAIXA.
114. As entregas terão garantia por um prazo mínimo de 90 (noventa) dias, contados a partir do aceite da CAIXA.
115. A CAIXA, a seu critério, fará abertura de chamado, convocará a CONTRATADA para, em reunião conjunta, fazer o planejamento de trabalho e ações a serem executadas com o objetivo de detalhar as atuações das respectivas equipes técnicas especializadas.
116. A CONTRATADA será responsável pela migração de todos os casos de uso existentes atualmente nas ferramentas de SIEM da CAIXA, LogRhythm para ambiente on premises e Microsoft Sentinel para o ambiente nuvem, seguindo as seguintes instruções:
- 116.1. Considerar o quantitativo de casos de uso a serem migrados de acordo com a sua complexidade descrito na Tabela 4.
- 116.2. Após o setup inicial da ferramenta, será agendado pela CAIXA reunião para estruturação e planejamento do projeto de migração dos casos de uso.
- 116.3. A CONTRATADA deverá realizar a migração dos casos de uso em um prazo de até 6 meses.
- 116.4. A CONTRATADA deverá disponibilizar equipe técnica e um Gerente ou Coordenador de Projetos para o acompanhamento das atividades ao longo do projeto.
- 116.5. Poderão ser aceitos casos de uso equivalentes na solução CONTRATADA, desde que mantenham o mesmo escopo e objetivo de monitoramento, e tenham sido validados pela CAIXA.

Quantidade de casos de uso a serem migrados de acordo com a complexidade			
	Alta	Média	Baixa
LogRhythm	0	2	21
Microsoft Sentinel	40	77	82
Total	40	79	103

Tabela 4 – Casos de uso por ambiente

- 117. Os casos de uso devem ser entregues, integrados à solução de gestão de incidentes cibernéticos definida pela CAIXA, salvo orientação contrária, e devidamente documentados, de acordo com padrão a ser acordado entre as partes.
- 118. A complexidade na elaboração de casos de usos e tamanho da demanda, para fins de categorização do serviço e definição do prazo de solução serão calculados de acordo com o esforço estimado, conforme parâmetros do ANEXO I-A – Forma de Execução do Contrato.

TREINAMENTO OFICIAL DA SOLUÇÃO DE GERENCIAMENTO E CORRELACIONAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) BASEADAS EM NUVEM (SAAS)

- 119. O treinamento oficial do fabricante deverá ser de, no mínimo, 40 (quarenta) horas e ministrado por Analista Certificado pelo Fabricante na solução ofertada;
- 120. O treinamento deverá ser realizado preferencialmente no modelo presencial;
- 121. O treinamento poderá ser realizado no modelo telepresencial (online por videoconferência), preferencialmente em português, utilizando ferramenta própria disponibilizada pela fabricante, de acordo com autorização da CAIXA;
- 122. A empresa deverá disponibilizar material aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento;
- 123. Caso não haja disponibilidade para realização nos modelos presencial ou telepresencial, a empresa deverá custear os gastos de passagens e estadia para o centro de treinamento mais próximo de Brasília.

ANEXO I-A**FORMA DE EXECUÇÃO DO CONTRATO****1 CONSIDERAÇÕES GERAIS**

- 1.1 A CAIXA indicará, formalmente, no ato da assinatura do CONTRATO, o(s) responsável(eis) pela gestão do CONTRATO e dos serviços contratados.
- 1.2 A CAIXA poderá indicar outro(s) responsável(eis), a qualquer momento, bastando apenas comunicar formalmente à CONTRATADA.
- 1.3 O relacionamento relativo à gestão do contrato será realizado nas dependências da CAIXA, exceto em situações excepcionais onde haja o entendimento e anuência da CAIXA para mudança de local.
- 1.4 A CONTRATADA deverá indicar, formalmente, no ato de assinatura do CONTRATO ou sempre que houver alteração/substituição, o(s) seu(s) representante(s) que será(ão) responsável(is) pelo acompanhamento da execução dos serviços contratados, atuando como Gerente(s) do Contrato.
- 1.5 A CONTRATADA deverá disponibilizar, sem custo adicional para a CAIXA, Gerente(s) de Serviços que será(ão) responsável(is) por garantir a qualidade dos serviços prestados, pelo acompanhamento dos chamados técnicos, pela emissão e entrega dos relatórios periódicos das atividades executadas, além da participação em reuniões sempre que convocado(s).
- 1.6 As funções de Gerente do Contrato e de Gerente de Serviços podem ser exercidas pelo(s) mesmo(s) profissional(is) da CONTRATADA, desde que essa condição não prejudique o perfeito atendimento às demandas da CAIXA.
- 1.7 As reuniões e demais atividades relacionadas ao planejamento, à gestão e à execução do contrato serão realizadas, preferencialmente, nas dependências da CAIXA, podendo ser realizada em formato remoto, mediante o entendimento e a anuência da CAIXA.
- 1.8 O acesso dos técnicos da contratada ou do fabricante dos produtos aos ambientes da CAIXA somente será admitido com prévia autorização e com observância aos padrões de segurança vigentes.
- 1.9 O acesso às informações do ambiente de produção do SIEM, a partir das instalações da CONTRATADA só será efetuado quando for possível restringir tal acesso apenas ao recurso objeto da contratação e em situações expressamente autorizada pela Caixa, obedecendo aos padrões em vigência na CAIXA.

- 1.10 A CONTRATADA se compromete a não divulgar dados ou informações relacionadas aos produtos objeto do presente contrato ou que venha a ter conhecimento durante a realização dos serviços, mantendo sigilo absoluto em relação aos dados acessados ou que venham a ser gerados, no processo de prestação dos serviços.
- 1.11 Para realização dos serviços especificados neste anexo, a CONTRATADA poderá utilizar ferramentas (software aplicativo) de sua propriedade, desde que autorizado pela CAIXA e destinado a facilitar a execução dos serviços e diagnósticos de problemas, sem ônus adicionais para a CAIXA.
- 1.12 Todas as despesas com mão de obra, deslocamentos, alimentação, estadia, hospedagem, impostos, encargos fiscais, encargos trabalhistas, margem de lucro e demais dispêndios que se fizerem necessários para a perfeita execução dos serviços contratados, em atendimento aos chamados técnicos ou em relação às demais atividades previstas, serão de exclusiva responsabilidade da CONTRATADA.
- 1.13 Todo serviço de suporte técnico deverá ser executado somente mediante prévia autorização da CAIXA, com informações claras dos procedimentos que serão adotados/executados, nos horários estabelecidos no Termo de Referência e demais anexos.
- 1.14 A CONTRATADA será responsável pela execução dos serviços e seu acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados por escrito a CAIXA.
- 1.15 Cabe à Contratada**
- 1.15.1 Manter consistentes e atualizados todos os artefatos produzidos e/ou disponibilizar acesso às informações relativas a problemas, falhas de segurança documentados pelo fabricante.
- 1.15.2 Manter documentação dos modelos alterados durante a execução dos serviços contratados.
- 1.15.3 Manter a consistência entre os modelos de dados adaptados e o modelo de dados corporativo da CAIXA.
- 1.15.4 Garantir que todas as entregas efetuadas estejam compatíveis e totalmente aderentes aos padrões tecnológicos utilizados pela CAIXA, cabendo à CAIXA

tomar ciência e autorizar o uso de produtos e/ou versões que sejam diferentes daqueles previstas e em uso na CAIXA.

- 1.15.5 Elaborar, sem ônus adicional para a CAIXA, toda a documentação necessária ao pleno conhecimento e operacionalização dos serviços de implantação, integração, desenvolvimento e serviço técnico especializado.

2 REGRAS DE ATENDIMENTO

- 2.1 O acionamento das equipes da CONTRATADA para a execução dos serviços de suporte técnico, implantação da solução, atualização tecnológica, administração, operação e serviços especializados, da solução de segurança SIEM, previstos neste contrato, se dará a partir da designação das requisições (chamados) por meio da ferramenta da CAIXA, mediante a disponibilização de ticket junto ao WebService/ITSM definido pela CAIXA.
- 2.2 Cabe à CONTRATADA a integração do seu sistema de atendimento com o da CAIXA.
- 2.3 Consiste em obrigação da CONTRATADA encaminhar o aceite de forma imediata quando da disponibilização do ticket respectivo no WebService/ITSM, quando solicitado pela CAIXA, bem como efetuar o fechamento dos chamados no instante da conclusão dos serviços com a imediata gravação dos tickets de fechamento no WebService/ITSM da CAIXA.
- 2.4 Para todos os efeitos e cálculos neste contrato, o prazo de solução dos chamados de atendimento inicia-se na data/hora em que for disponibilizado a partir dos sistemas da CAIXA o ticket no WebService/ITSM ou, no caso de se tratar de demanda com horário de intervenção necessariamente agendado pela CAIXA, iniciar-se-á na data e hora agendada, encerrando-se a contagem do prazo de solução, para ambos os casos, na data e hora em que o ticket de conclusão da CONTRATADA, disponibilizado por esta no WebService/ITSM da CAIXA, for sensibilizado neste ou em outra ferramenta que a CAIXA venha a utilizar.
- 2.5 Os dados oficiais para cálculo de SLA e respectivos descontos serão os dados baseados na integração do sistema da CAIXA com a CONTRATADA.
- 2.6 Em caso de indisponibilidade dos sistemas da CAIXA ou da CONTRATADA, poderão ser utilizados, a critério exclusivo da CAIXA, outros canais para encaminhar os chamados ou receber o fechamento contingencial, tais como e-mail protocolado, e-mail, serviço 0800 ou contato telefônico.
- 2.7 A CAIXA apresentará, após a assinatura do contrato, o layout dos registros dos bilhetes/tickets (abertura, aceite, atualizações e conclusão) e a CONTRATADA terá um prazo de 30 (trinta) dias corridos, contados a partir da disponibilização

do layout, para desenvolvimento, testes e implementação da integração dos sistemas de atendimentos das partes.

- 2.7.1 Durante o período inicial de integração dos sistemas (30 dias corridos), para o período em questão, os descontos serão baseados nos dados da CAIXA mediante negociação com a CONTRATADA.
- 2.7.2 Caso a CONTRATADA não cumpra o prazo de integração valerão os dados da CAIXA de forma sumária.
- 2.7.3 Em caso de alteração do layout dos tickets/bilhetes, a CONTRATADA terá o prazo de **15 (quinze) dias corridos** para adequar sua ferramenta de WebService/ITSM para a devida recepção deles, a partir do momento da notificação de alteração e entrega do novo leiaute.
- 2.7.4 O atraso na integração e/ou nas adequações, com base nos prazos definidos acima, ensejará em aplicação de multas à CONTRATADA.
- 2.7.5 Estará sujeita a multa de 0,09% (nove centésimos por cento) por dia corrido de atraso, limitado a 10% (dez por cento), a ser calculado sobre o valor da fatura mensal do período corrente.
- 2.7.6 É obrigação da CONTRATADA, às suas expensas, a conexão dedicada para a troca de tickets com o WebService/ITSM disponibilizado pela CAIXA devendo adequar-se ao padrão utilizado por esta.
- 2.7.7 Os chamados abertos e/ou demandas encaminhadas deverão ser tratados com atendimento em português, com escalação e acompanhamento em tempo real.
- 2.7.8 A CONTRATADA deverá informar, em até **5 (cinco) dias** após assinatura do contrato, pelo menos uma caixa postal para acionamento e recebimento de mensagem eletrônica e um número de telefone para contingenciamento em caso de indisponibilidade da central de atendimento.
- 2.7.9 O termo forma corrido indica que a contagem de tempo se dará de maneira contínua sem interrupções, exceto aqueles que sejam provocados pela CAIXA.
- 2.7.10 A CONTRATADA deverá fornecer relatório detalhado, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico, em português, referente as atividades prestadas, contendo dados gerenciais e estatísticos pertinentes à gestão dos serviços relativos ao mês anterior, cujo padrão e modelo incluirão, obrigatoriamente, os itens relacionados a seguir e poderão sofrer alterações conforme necessidade da CAIXA, acordados com a CONTRATADA:
- Data e hora de abertura do chamado técnico

- Identificação da unidade CAIXA
- Nome do responsável pela abertura do chamado
- Severidade do chamado
- Número identificador do chamado
- Data e hora de início do atendimento
- Data e hora da conclusão da solução operacional
- Data e hora da solução definitiva do chamado
- Data e hora da conclusão definitiva do chamado
- Detalhamento do tempo em que a ação ficou sob responsabilidade da CAIXA
- Quantidade de ocorrências (chamados) registradas no período
- Informações sobre eventuais escalações
- Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido
- Total de chamados no mês e o total acumulado até a apresentação do relatório

2.7.10.1 Este relatório é uma obrigação contratual sujeita às sanções previstas no item 5 – CÁLCULO DO NÍVEL DE SERVIÇO E SANÇÕES, o qual deverá ser entregue no local de execução do contrato, conforme item 7 – LOCAL DE EXECUÇÃO.

2.7.11 A qualidade dos serviços será aferida na forma estabelecida no item 5 – CÁLCULO DO NÍVEL DE SERVIÇO E SANÇÕES.

3 VIGÊNCIA CONTRATUAL

3.1 O prazo para a prestação dos serviços objeto deste Termo de Referência será de 36 (trinta e seis) meses, contados da data de sua assinatura, podendo ser prorrogado, a critério da CAIXA e com a concordância da CONTRATADA, até o limite permitido na legislação.

4 FORMA DE REMUNERAÇÃO DOS SERVIÇOS

4.1 A CAIXA realizará a remuneração dos serviços da seguinte forma:

4.2 O período de migração/implantação dos casos de uso deverá ocorrer em até 6 meses, podendo ser prorrogado mediante aceite da CAIXA.

4.3 O pagamento será mensal de acordo com o volume de dados ingeridos, em GB/dia, na ferramenta.

4.4 Ao final da implantação, o pagamento se dará conforme uso da solução de SIEM.

4.5 Na hipótese de atraso na entrega dos casos de uso será aplicado desconto de 0,1%, por caso de uso, na fatura mensal, a cada mês de atraso.

- 4.6 Quantidade de casos de uso e Tecnologias utilizadas atualmente que deverão ser migradas para o novo serviço de SIEM:

Quantidade de casos de uso a serem migrados de acordo com a complexidade			
	Alta	Média	Baixa
LogRhythm	0	2	21
Microsoft Sentinel	40	77	82
Total	40	79	103

2000 GB/DIA UTILIZADOS ATUALMENTE	
TECNOLOGIAS	PERCENTUAL % DE INGESTÃO
Microsoft Defender for Endpoint	46,50
Active Directory	21,41
Cisco ASA	8,82
Oracle SunOne Directory Server	6,60
Azure - Syslog	4,31
Microsoft Defender for Cloud Apps	3,83
Mainframe z/OS events	2,07
Single Sign-On	1,51
McAfee Web Gateway	1,16
Microsoft Defender for Office 365	1,01
OpenLDAP	1,01
Microsoft Defender for Identity	0,60
Azure Active Directory	0,43
Azure Firewall e outros	0,25
Microsoft Forefront TMG	0,25
Cisco ISE	0,15
Microsoft DHCP Server Log	0,05
Bind DNS	0,05
TOTAL	100,00

- 4.7 O período de faturamento será compreendido entre o primeiro e o último dia de cada mês.
- 4.8 A CAIXA, após a aceitação dos serviços, efetuará o pagamento a CONTRATADA, mensalmente, no 15º, (décimo-quinto) dia útil do mês subsequente ao da efetiva execução dos serviços, mediante crédito em conta corrente mantida pela CONTRATADA, obrigatoriamente em agência da CAIXA, devendo a emissão da correspondente nota fiscal ser antecipada, com apresentação à CAIXA, impreterivelmente, até o 10º (décimo) dia útil do mês subsequente ao da efetiva execução dos serviços, prorrogando-se o prazo de pagamento na mesma proporção de eventual atraso ocorrido na entrega da fatura.

5 CÁLCULO DO NÍVEL DE SERVIÇO E SANÇÕES

- 5.1 O Nível de Serviço é um indicativo de qualidade da prestação do serviço.
- 5.2 A qualidade da prestação de serviços será apurada por meio de Indicadores, cuja finalidade é garantir o atendimento célere aos chamados, bem como a sua correta priorização.
- 5.3 Para garantir a adequação contínua dos serviços às necessidades dos negócios da CAIXA, bem como em decorrência da evolução tecnológica a CAIXA poderá propor a revisão de indicadores. Uma vez que tais propostas sejam aceitas pela CONTRATADA, o novo conjunto passará a ser considerado a partir da data acordada por ambas as partes.
- 5.4 A qualidade da prestação de serviços será apurada por meio de indicadores, cuja finalidade é garantir o atendimento célere aos chamados, relatórios obrigatórios, bem como a sua correta priorização.
- 5.5 Os descontos serão cumulativos para cada dia, hora ou fração de atraso de cada chamado fechado no mês de referência de acordo com sua severidade e deverão ser aplicados na fatura do mês seguinte ao período de apuração.
- 5.6 Para o último mês de vigência do contrato a apuração deverá ser antecipada de maneira que os descontos sejam aplicados na última fatura do contrato.
- 5.7 A CONTRATADA, imediatamente após receber o chamado da CAIXA, deverá prover atendimento e solução nos prazos estabelecidos neste item.

5.8 INDICADORES**5.8.1 Serviços de SIEM**

- 5.8.1.1 Pela inobservância de quaisquer exigências estabelecidas no ANEXO I – Termo de Referência – Especificação Técnica, a CONTRATADA estará sujeita a um desconto na fatura do período de 0,02% (dois centésimos por cento) por dia corrido de atraso e por ocorrência (subitem descumprido), a ser calculado sobre o valor da fatura mensal do período corrente.

5.8.2 Suporte técnico, Administração e Operação

- 5.8.2.1 Descrição das severidades dos indicadores de incidentes da infraestrutura de SIEM:

Severidade	Descrição
------------	-----------

1 – Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade de sistema. A solução não está operante e não é possível nenhuma solução de contorno viável.
2 – Alta	Um ou mais componentes da solução parcialmente indisponíveis, causando indisponibilidade de funcionalidades, com alguns serviços funcionando.
3 – Média	Um ou mais componentes da solução apresentam erros ou alertas que não causam indisponibilidade das suas funcionalidades.
4 – Baixa	Demais incidentes que possam comprometer a infraestrutura do SIEM.

5.8.2.2. Tempo máximo de início de atendimento aos incidentes no SIEM:

TMIA – Tempo máximo de início de atendimento aos incidentes no SIEM		
Item	Tempo máximo para início do atendimento: tempo máximo requerido para o início do atendimento à solução.	
Finalidade	Garantir o início do atendimento conforme prazo acordado.	
Meta a cumprir	Severidade	Tempo previsto
	1 – Crítica	15 min
	2 – Alta	30 min
	3 – Média	2 horas
	4 – Baixa	4 horas
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	TMIA = Considera-se a duração do atraso de cada chamado, que será calculado por meio da fórmula: (Data/hora fim do início do atendimento – data/hora início do chamado).	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	TMIA	0,25% de desconto na fatura mensal por hora (ou fração) da duração de atraso de cada chamado.
Observações	Quando a duração do atraso não for múltiplo exata de hora, será arredondado para múltiplo imediatamente superior.	

5.8.2.3. Tempo máximo de solução operacional aos incidentes no SIEM:

TMSO – Tempo máximo de solução operacional relacionados a infraestrutura de SIEM
--

Item	Tempo máximo de solução operacional: tempo máximo requerido para contornar o problema e deixar o sistema/serviço disponível	
Finalidade	Garantir a solução operacional conforme prazo acordado	
Meta a cumprir	Severidade	Tempo previsto
	1 – Crítica	4 horas
	2 – Alta	8 horas
	3 – Média	16 horas
	4 – Baixa	24 horas
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	TMSO = Considera-se a duração do atraso de cada chamado, que será calculado por meio da fórmula: $((\text{Data/hora fim da solução operacional} - \text{data/hora início do chamado}) - \text{tempo sob responsabilidade da CAIXA})$	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	1 – Crítica	0,5% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	2 – Alta	0,4% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	3 - Média	0,2% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	4 - Baixa	0,1% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
Observações	Quando a duração do atraso não for múltiplo exato de hora, será arredondado para múltiplo imediatamente superior.	

5.8.2.4. Tempo máximo de solução definitiva do chamado de incidente no SIEM:

TMSDC – Tempo máximo de solução definitiva do chamado de incidente relacionados a infraestrutura de SIEM		
Item	Tempo máximo de solução definitiva do chamado: tempo máximo requerido para solucionar em definitivo a causa do problema, calculado a partir da abertura do chamado	
Finalidade	Garantir a solução definitiva conforme prazo acordado	
Meta a cumprir	Severidade	Tempo previsto
	1 – Crítica	24 horas

	2 – Alta	36 horas
	3 – Média	48 horas
	4 – Baixa	72 horas
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	TMSDC = Considera-se a duração do atraso de cada chamado, que será calculado por meio da fórmula: ((Data/hora fim da solução definitiva – data/hora início do chamado) – tempo sob responsabilidade da CAIXA)	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	1 – Crítica	0,05% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	2 – Alta	0,025% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	3 - Média	0,020% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
	4 - Baixa	0,015% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado.
Observações	Quando a duração do atraso não for múltipla exata de hora, será arredondado para múltiplo imediatamente superior.	

5.8.2.5. Tempo máximo para esclarecimento de dúvidas sobre o SIEM:

TMED – Tempo máximo para esclarecimento de dúvidas relacionados a infraestrutura de SIEM		
Item	Tempo máximo requerido para esclarecimento de dúvidas sobre os produtos; chamados para correções e parametrizações; e consultas técnicas.	
Finalidade	Garantir o esclarecimento de dúvidas sobre os produtos e consultas técnicas conforme prazo acordado	
Meta a cumprir	Tempo previsto	48 horas
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	

Mecanismo de cálculo	TMED = Considera-se a duração do atraso de cada chamado, que será calculado por meio da fórmula: (Data/hora fim do chamado/requisição – data/hora início do chamado/requisição).	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	TMED	0,1% de desconto na fatura mensal por hora (ou fração) da duração do atraso de cada chamado/requisição.
Observações	Quando a duração do atraso não for múltipla exata de hora, será arredondado para múltiplo imediatamente superior.	

5.8.2.6. Tempo máximo para fornecimento de relatório consolidado dos chamados referentes a infraestrutura do SIEM:

Fornecimento de relatório consolidado dos chamados relacionados a infraestrutura de SIEM		
Item	Tempo máximo requerido para entrega do relatório consolidado dos chamados	
Finalidade	Garantir a entrega do relatório consolidado dos chamados	
Meta a cumprir	Entrega do relatório	5º dia útil do mês subsequente à prestação do serviço
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	(TMRCC) Conferência da data de entrega do relatório em conformidade com todas as especificações e dados exigidos.	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	Entrega	0,1% de desconto no valor global do contrato por dia de atraso.
Observações	-	

5.8.3 Serviços de suporte a solução

5.8.3.1. Descrição do esforço estimado nas demandas dos serviços de suporte a solução:

DESCRIÇÃO DOS SERVIÇOS				
SERVIÇO	DESCRIÇÃO	MULTIPLICADOR	COMPLEXIDADE	TEMPO DE ATENDIMENTO EM HORAS

Desenvolvimento de parsers customizados	Desenvolver parsers que consigam identificar padrões nos logs não padronizados que chegam na solução de SIEM de forma a tornar esses campos indexáveis pela solução.	1	Baixa	96
		3	Média	
		5	Alta	
Desenvolvimento de scripts	Desenvolver scripts para integrar os alertas gerados na solução de SIEM com a solução de gerenciamento de incidentes cibernéticos da CAIXA ou outros scripts necessários na solução de SIEM.	1	Baixa	48
		3	Média	
		5	Alta	
Desenvolver regras de negócios especificadas pela CAIXA que irão compor os casos de uso	Desenvolver regras de correlação, filtragem, exclusão, agrupamento, ou duração para construção dos casos de uso especificados pela CAIXA	1	Baixa	48
		3	Média	
		5	Alta	
Criação e customização de relatórios personalizados	Criação e customização de relatórios personalizados, de acordo com a necessidade da CAIXA que não são facilmente criados com os parâmetros definidos previamente na solução	1	Baixa	72
		3	Média	
		5	Alta	
Desenvolvimento e customização de Playbooks	Desenvolver e customizar Playbooks para automatizar os processos de geração de alarme no	1	Baixa	96
		3	Média	
		5	Alta	

	tratamento de incidente cibernético			
Desenvolvimento e customização de integração com base de dados SQL ou NoSQL	Desenvolvimento e customização de integração com base de dados estruturadas ou não estruturadas com o objetivo de importação desses dados para a solução SIEM	1	Baixa	48
		3	Média	
		5	Alta	

5.8.3.2. Descrição dos fatores de complexidade

FATORES DE COMPLEXIDADE		
COMPLEXIDADE	DESCRIÇÃO DAS ATIVIDADES	MULTIPLICADOR
Baixa	Desenvolvimento de parsers, scripts ou regras de negócios de casos de uso de baixa complexidade, que na maioria das vezes são parametrizadas na solução; OU customizações de relatórios, customizações de playbook e integração de base de dados que não exigem um esforço complexo na construção.	1
Média	Desenvolvimento de parsers, scripts ou regras de negócios de casos de uso de média complexidade, que podem, em pequena parte ser parametrizados na solução, mas exigirá um esforço adicional de desenvolvimento; OU customizações de relatórios, customizações de playbook ou integração de base de dados que podem exigir um esforço de desenvolvimento na construção.	3
Alta	Desenvolvimento de parsers, scripts ou regras de negócios de casos de uso de alta complexidade, com necessidade comercial muito mais complexa que o usual, requerendo conhecimento de especialistas; OU customizações de relatórios, customizações de playbook e integração de base de dados que exigem grande esforço no desenvolvimento da solução;	5

- 5.8.3.3. Devido a evolução tecnológica da solução e a diversidade de componentes, o rol das atividades descritas não é exaustiva e poderá ser ajustado no decorrer do contrato.
- 5.8.3.4. Tempo máximo para atendimento das demandas definidas pela CAIXA nos serviços de suporte a solução

Tempo máximo para atendimento das demandas definidas pela CAIXA nos serviços de suporte a solução		
Item	Tempo máximo para atendimento das demandas definidas pela CAIXA nos serviços de suporte a solução	
Finalidade	Atendimento das demandas de serviços de suporte	
Meta a cumprir	Complexidade	Tempo previsto Tempo de atendimento em horas x Multiplicador de complexidade ex.: (96*1, 72*3, 48*5)
	Alta	
	Média	
	Baixa	
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir	
Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	Considera-se a duração do atraso de cada chamado, que será calculado por meio da fórmula: ((Data/hora fim do atendimento – data/hora início do atendimento) – tempo sob responsabilidade da CAIXA)	
Início da vigência	Data da assinatura do contrato	
Faixa de ajuste no pagamento	0,04% de desconto no pagamento do serviço especializado sob demanda, por dia (ou fração) da duração do atraso de cada chamado.	
Observações	Quando a duração do atraso não for múltipla exata de um dia, será arredondado para múltiplo imediatamente superior.	

- 5.8.3.5. Quantidade de defeitos nos serviços entregues

Defeitos nos serviços entregues	
Item	Quantidade de chamados abertos para corrigir um serviço especializado
Finalidade	Garantir qualidade nas entregas dos serviços especializados
Meta a cumprir	0 (zero) defeitos
Instrumento de medição	Procedimentos, rotinas, ferramentas de gerenciamento adotadas pela CAIXA ou que a CAIXA vier a definir

Forma de acompanhamento	Por intermédio dos instrumentos de medição	
Periodicidade	Mensal	
Mecanismo de cálculo	Quantidade de chamados abertos no período para correção de defeitos dos serviços especializados entregues	
Início da Vigência	Após a fase de inicialização do contrato	
Faixa de ajuste no pagamento	$x \leq 0$	0,000%
	$0 < x \leq 2$	0,300%
	$2 < x \leq 4$	0,400%
	$4 < x \leq 6$	0,600%
	$X > 6$	0,900%
Base de cálculo	Valor da fatura mensal do respectivo período	

- 5.9. Considera-se um problema definitivamente solucionado quando os serviços relacionados à solução forem restabelecidos sem restrições e de forma plena, ou seja, quando não se tratar de uma solução de contorno (workaround).
- 5.10. Os prazos estabelecidos para fechamento dos atendimentos não se aplicam a ocorrências que, pela sua natureza, envolverem atividades relacionadas a desenvolvimento de patches específicos, admitindo-se para todos os casos a adoção de solução de contorno (workaround). Para a solução de contorno devem ser respeitados os prazos definidos para cada severidade informada.
- 5.11. Em caso de impossibilidade de fechamento do atendimento dentro dos prazos estabelecidos, a CONTRATADA deverá, ainda dentro dos prazos definidos, emitir um parecer com previsão do novo prazo para atendimento da demanda, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a abertura do respectivo chamado/requisição.
- 5.12. Após a avaliação deste parecer, a CAIXA decidirá sobre a periodicidade da emissão de pareceres ou laudos posteriores, até o fechamento final do atendimento.
- 5.13. No descumprimento de atendimento aos níveis de serviços, a contratada será penalizada conforme definido no item 5 deste anexo.
- 5.14. Pelo não cumprimento das obrigações assumidas, garantida a previa defesa em processo regular, a CONTRATADA sujeitar-se-á às seguintes sanções, sem prejuízo das demais cominações aplicáveis:
- multa;
 - suspensão temporária de participar em licitação e impedimento de contratar com a CAIXA;
 - declaração de inidoneidade para licitar e contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até

que seja promovida a reabilitação perante a própria autoridade que aplicou a pena;

- 5.15. Para o descumprimento de quaisquer outras obrigações contratuais será aplicado multa no valor de 0,1% (um décimo por cento) do valor da fatura mensal, por dia de atraso que perdurar o descumprimento, exceto quando a resolução depender de ação da CAIXA.
- 5.16. As multas serão descontadas do valor da garantia contratual, da fatura ou cobradas diretamente da CONTRATADA ou judicialmente.
- 5.17. Se a multa for de valor superior ao valor da garantia apresentada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CAIXA ou ainda, quando for o caso, cobrada judicialmente.
- 5.18. A penalidade de declaração de suspensão temporária de licitar e contratar com a CAIXA pelo prazo de até 05 (cinco) anos poderá ser aplicada em casos de reincidências, em descumprimento de prazo contratual, descumprimento parcial ou total de obrigação contratual ou, ainda, em caso de rescisão contratual, mesmo que desses fatos não resulte prejuízo à CAIXA.
- 5.19. A penalidade de declaração de inidoneidade poderá ser proposta se a CONTRATADA:
- a) descumprir ou cumprir parcialmente obrigação contratual, desde que desses fatos resultem prejuízos à CAIXA;
 - b) sofrer condenação definitiva por prática de fraude fiscal no recolhimento de quaisquer tributos, ou deixar de cumprir suas obrigações fiscais ou parafiscais;
 - c) tiver praticado atos ilícitos visando frustrar os objetivos da licitação.
- 5.20. As penalidades de suspensão temporária e de declaração de inidoneidade, aplicadas pela competente autoridade da CAIXA ou ministerial, respectivamente, após a instrução do pertinente processo, no qual fica assegurada a ampla defesa da CONTRATADA, serão lançadas no SICAF.
- 5.21. A penalidade de declaração de inidoneidade implica a inativação do cadastro no SICAF, impossibilitando o fornecedor ou interessados de relacionar-se com a Administração Pública Federal e demais órgãos/entidades integrantes desse Sistema.
- 5.22. A falta de quaisquer dos materiais cujo fornecimento e manutenção incumbe à CONTRATADA, não poderá ser alegada como motivo de força maior para o atraso, má execução ou inexecução do fornecimento objeto deste contrato e

não a eximirá das penalidades a que está sujeita pelo não cumprimento dos prazos e demais condições estabelecidas.

- 5.23. Caso a CAIXA não se utilize da prerrogativa de rescindir o contrato a seu exclusivo critério, poderá suspender a sua execução, suspendendo o pagamento da respectiva fatura, até que a CONTRATADA cumpra integralmente a condição contratual infringida.
- 5.24. O descumprimento das obrigações relacionadas com confidencialidade e segurança de dados, de informações e sistemas, mediante ações ou omissões, intencionais ou acidentais, que impliquem em perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenados, em que trafeguem ou do ambiente em que estejam sendo processados, determinará a responsabilização, na forma da lei, de seus dirigentes e funcionários envolvidos.

6 TRANSFERÊNCIA DE CONHECIMENTO

- 6.1 Deverá ser disponibilizado para a CAIXA treinamentos de até 5 (cinco) turmas de 15 (quinze) pessoas (sob demanda), durante a execução do contrato.
- 6.2 Os treinamentos deverão possuir conteúdos suficientes para que o treinando passe a conhecer os produtos ora fornecidos neste contrato, seu funcionamento e sua arquitetura de modo a estarem aptos a:
- Implementar suas funcionalidades e configurá-las de forma a atender às necessidades da Caixa;
 - Avaliar situações que envolvam aspectos de performance /desempenho propondo ações de melhoria;
 - Realizar o planejamento de capacidade e desempenho.
- 6.3 A critério da CAIXA a turma poderá ser presencial ou remota, e deverão ser ministrados em Brasília com turma mínima de **5 (cinco)** pessoas.
- 6.4 Ao final de cada evento, os participantes com o mínimo de 80% (oitenta por cento) de presença deverão receber certificados de participação, e ainda:
- 6.4.1 Deverá ser realizada pesquisa de satisfação entre os participantes.
- 6.4.2 Caso o curso não atinja a avaliação mínima, como de nível satisfatório, a contratada deverá tomar providências de realização de nova transferência de conhecimento dentro de um prazo de até **45 (quarenta e cinco) dias**.
- 6.5 A CAIXA emitirá, em até **10 (dez) dias úteis** após o final da realização das atividades de transferência de conhecimento, um Termo de Aceite da transferência de conhecimento.

7. ENCERRAMENTO DO CONTRATO

- 7.1. A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.
- 7.2. A Contratada deverá disponibilizar os backups de dados e configurações dos casos de uso implantados na ferramenta por no mínimo 90 dias antes do encerramento do contrato.
- 7.3. A Contratada deve reter os dados por até 90 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.
- 7.4. Portanto, a CAIXA poderá avaliar durante esse período que compreende no total 180 dias, a melhor maneira de realizar a migração dos dados e configurações relacionadas.
- 7.5. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.
- 7.6. A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

8. LOCAL DE EXECUÇÃO

- 9.1. Os serviços contratados, descritos no objeto deste Termo de Referência, serão realizados nas dependências da CAIXA, na seguinte localidade:

CESET – CENTRALIZADORA NACIONAL SEGURANÇA CIBERNÉTICA
ASA NORTE
BRASILIA – DF | CEP 70760-706

- 7.1.2. A CAIXA se reserva ao direito de alterar os locais de execução dos serviços, de acordo com suas necessidades, sem ônus adicionais para a CAIXA.
- 7.1.3. Qualquer mudança de local, que venha a implicar em alteração de endereço, cidade ou estado, deverá ser comunicada pela CAIXA à CONTRATADA, com no mínimo 30 (trinta) dias corridos antes da efetiva mudança.
- 7.1.4. A CONTRATADA deverá ajustar seus processos, realocar seus recursos e pessoas no período de 5 (cinco) dias úteis após a efetiva mudança.

8. UNIDADE RESPONSÁVEL PELA GESTÃO E FISCALIZAÇÃO DO CONTRATO

8.1 Aspectos financeiros do contrato, tais como: faturamento, consolidação das contestações e aplicações de descontos, glosas e multas, bem como outras atividades pertinentes à gestão econômico-financeira serão realizadas pela CESET – CENTRALIZADORA NACIONAL SEGURANÇA CIBERNÉTICA ou outra unidade que a CAIXA venha a definir.

8.2 Unidade responsável pela gestão e fiscalização do contrato:

CESET – CENTRALIZADORA NACIONAL SEGURANÇA CIBERNÉTICA
ASA NORTE
BRASILIA – DF | CEP 70760-706

ANEXO I-B**REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES DE NUVEM****1. REQUISITOS DE NUVEM**

- 1.1. A CAIXA entende como PROVEDOR DE SERVIÇOS EM NUVEM, as empresas que disponibilizam serviços em nuvem pública ou privada sob demanda em hiperescala. A hiperescala é a capacidade de uma arquitetura ser dimensionada de forma adequada conforme a demanda é aumentada e adicionada ao serviço.
- 1.2. Os serviços em nuvem consistem em infraestrutura como Serviço (IaaS), plataforma como Serviço (PaaS) e Software como Serviço (SaaS).
- 1.3. O PROVEDOR deverá fornecer os serviços de computação em nuvem em aderência seguintes princípios elencados pelo NIST:
- 1) Auto-provisionamento sob demanda (“on-demand self-service”): o consumidor pode ter a iniciativa de provisionar recursos na nuvem, e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços.
 - 2) Acesso amplo pela rede (“broad network access”): os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (tais como: estações de trabalho, tablets e smartphones) através de mecanismos padrões.
 - 3) Compartilhamento através de pool de recursos (“resource pooling”): Os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo multi-tenant), com recursos físicos e virtuais sendo alocados e realocados dinamicamente, de acordo com a demanda dos seus consumidores. Há uma ideia geral de independência de localização, uma vez que o cliente geralmente não possui controle ou conhecimento sobre a localização exata dos recursos providos. No entanto, é possível especificar este local em um nível mais alto de abstração (por exemplo: país, estado ou data center). Os serviços são concebidos como um padrão, com a finalidade de atender à demanda de vários consumidores de maneira compartilhada, não sendo focados em necessidades customizadas de um único consumidor.
 - 4) Rápida elasticidade: os recursos podem ser elasticamente provisionados e liberados, e, em alguns casos, de maneira automática, adaptando-se à demanda. Do ponto de vista do consumidor, os recursos disponíveis para provisionamento parecem ser ilimitados, podendo ser alocados a qualquer hora e em qualquer volume.

5) Serviços medidos por utilização (“measured service”): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado (por exemplo: armazenamento, processamento, largura de banda, e contas de usuário ativas). A utilização dos recursos pode ser monitorada, controlada e reportada, fornecendo transparência tanto para provedores como para consumidores. Portanto, a precificação, se houver, será balizada pelo uso dos serviços.”

- 1.4. Os requisitos deste capítulo se aplicam às empresas que prestarão serviços em nuvem para a CAIXA, ou que irão manter a estrutura de atendimento para a CAIXA em nuvem pública, incluindo o armazenamento de arquivos corporativos que tenham relação com o trabalho desempenhado na CAIXA. As empresas Contratadas para prestação de serviços em nuvem também devem observar os controles relatados nos demais capítulos deste documento.
- 1.5. Os serviços em nuvem do tipo SaaS poderão ser provenientes tanto do marketplace ou do catálogo de serviços do provedor de nuvem, oriundos de um contrato de Multinuvem e fornecidos pelo provedor; quanto serviços de SaaS contratados a parte e provenientes de contratos específicos com a empresa fornecedora da solução.

2. Gestão de Identidade e Controle de Acessos

- 2.1. A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.
- 2.2. A Contratada deve manter rígido controle de acesso de seus colaboradores baseado nas informações de contratação, dispensa e controle de ausências (férias, licenças, atestados, admissão, demissão etc.) impedindo o acesso ao ambiente computacional, local ou remoto, quando o colaborador não estiver em pleno exercício de suas atividades.
- 2.3. A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 2.4. A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos

fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

- 2.5. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 2.6. Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.
- 2.7. As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 2.8. Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 2.9. A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 2.10. A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 2.11. A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.
- 2.12. Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.
- 2.13. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 2.14. A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 2.15. A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.
- 2.16. A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

- 2.17. A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 2.18. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 2.19. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.
- 2.20. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.
- 2.21. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 2.22. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.
- 2.23. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:
O tipo de evento (inclusão, alteração, exclusão, consulta);
O autor do evento;
A data e hora do evento;
O endereço lógico do equipamento de origem do tipo do evento.
- 2.24. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 2.25. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.
- 2.26. Devem ser observadas as boas práticas de segregação e diferenciação entre ambientes de não produção e produtivo, estabelecendo-se acessos

pertinentes para cada etapa do ciclo de desenvolvimento/manutenção e alinhado com o princípio do privilégio mínimo.

- 2.27. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 2.28. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.
- 2.29. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos na seção 2.4.
- 2.30. A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

3. Controles Criptográficos

- 3.1. Os requisitos apresentados nesta seção devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá comprovar por relatório de auditoria (Due Dilligence Remoto) que o armazenamento/processamento dos dados ocorre somente em ambiente de nuvem e o Provedor deve atender, além dos requisitos a seguir, as regras descritas no item 6 deste Guia.
- 3.2. A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.
- 3.3. A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.

- 3.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 3.5. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 3.6. A Contratada deve fazer a geração e a renovação de certificados digitais expostos na Internet junto a autoridades certificadoras reconhecidas internacionalmente, cujas raízes de cadeias utilizadas na emissão dos certificados digitais façam parte do repositório de cadeias confiáveis dos principais navegadores e versões de sistemas operacionais, como: iOS 7 e superiores; Android 4 e superiores; Microsoft Edge 12 e superiores; Mozilla Firefox 45 e superiores; Google Chrome 49 e superiores; Apple Safari 8 e superiores; Linux Ubuntu 14 e superiores; Linux Mint 15 e superiores; MAC OS X 10.10 e superiores; e Windows 7 e superiores.
- 3.7. A Autoridade Certificadora deve possuir o selo Web Trust dentro do prazo de validade e a certificação Web Trust deve estar de acordo com, no mínimo, os Princípios e Critérios para Autoridades Certificadoras – versão 2.2.1, disponível em <https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt100awebtrust-for-ca-221-110120-finalaoda.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6FD> para todas as raízes de cadeias utilizadas na emissão dos certificados digitais.
- 3.8. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).
- 3.9. As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 3.10. Caso haja a necessidade do compartilhamento de chaves simétricas entre a CAIXA e a Contratada, essas chaves devem ser geradas pela CAIXA e levadas para o ambiente da Contratada, onde devem ser armazenadas por meio de soluções FIPS 140-2 nível 3, sem possibilidade de exportação das chaves. Nesse caso, a Contratada deve prover meios que permitam a inserção das chaves da CAIXA no seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

- 3.11. No caso de utilização de um Provedor de Serviços em Nuvem, as certificações FIPS exigidas estão descritas na seção 6.
- 3.12. A Contratada deve permitir a criptografia de dados em repouso, considerando volumes (por exemplo: a criptografia de um disco inteiro) e estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).
- 3.13. A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.
- 3.14. A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.
- 3.15. A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.
- 3.16. A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.
- 3.17. A Contratada deve permitir a auditoria da segurança de chaves criptográficas.
- 3.18. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3, ou, quando não for suportado, 1.2.
- 3.19. A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.2 e as cifras a seguir:
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- 3.20. Os parâmetros TLS Renegotiation e TLS Resumption devem estar desabilitados.
- 3.21. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão mTLS, por exemplo – a Contratada deve fazer todas as

validações previstas no método X509_verify_cert, existente na estrutura do Openssl.

- 3.22. O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.

4. CONTROLE DE ACESSO AO AMBIENTE DE NUVEM

- 4.1. Quando viável tecnicamente, o acesso de empregados CAIXA à nuvem deverá ser integrado com ferramenta de SSO da CAIXA, ou com o AD, para garantir o uso das credenciais internas, isso deve garantir que o usuário não acesse o ambiente do parceiro, caso seja desligado ou esteja ausente da CAIXA por qualquer motivo por período determinado.
- 4.2. Como apresentado no item 2.4, quando a autenticação for provida pela Contratada ou pelo Provedor de Serviços em Nuvem, deverá ser realizada autenticação por múltiplos fatores para o acesso dos empregados da CAIXA, que precisem acessar os recursos em nuvem.
- 4.3. O acesso aos recursos da CAIXA deverá ser realizado em tenant designado especificamente, sem que estes recursos sejam compartilhados com qualquer outra entidade, bem como a camada de dados da aplicação não pode ser compartilhada com outros clientes do Provedor de Serviços em Nuvem.
- 4.4. O Provedor de Serviços em Nuvem deve permitir que somente os usuários autorizados pela CAIXA tenham acesso aos recursos em conformidade aos respectivos perfis de uso.
- 4.5. Os acessos administrativos aos recursos do Provedor de Serviços em Nuvem, nos tenants que atendam à CAIXA, deverão ser feitos através de rede privada, tanto para empregados CAIXA quanto para representantes do Provedor.

5. REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

- 5.1. A Contratada deve garantir que a prestação dos serviços não causará prejuízo ao funcionamento regular da CAIXA nem embaraço à atuação da Banco Central do Brasil, assegurando que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços serão prestados não restringem nem impedem o acesso da CAIXA nem do Banco Central do Brasil aos dados e às informações.

- 5.2. A Contratada deve assegurar que os dados sujeitos a limites geográficos não serão migrados para além das fronteiras definidas em contrato, incluindo dados de backup, dados em produção, dados em repouso, contingência ou recuperação de desastre sem prévio conhecimento da CAIXA por meio comunicação formal.
- 5.3. Deve ainda garantir acesso à CAIXA, a qualquer tempo, aos dados e às informações processadas, armazenadas e geradas pela atividade de processamento, Log, sob responsabilidade da Contratada;
- 5.4. Esta mesma Contratada deve assegurar que os dados da CAIXA processados e armazenados na Contratada são de propriedade exclusiva da CAIXA.
- 5.5. A Contratada deve assegurar também que o acesso aos dados processados e armazenados na Contratada é de acesso exclusivo da CAIXA, não sendo autorizado acesso da Contratada ou terceiros sem autorização formal da CAIXA.
- 5.6. A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.
- 5.7. Também deve assegurar à CAIXA acesso aos relatórios e documentos elaborados por empresa de auditoria especializada independente, contratada pelo provedor de serviço em nuvem, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados a qualquer tempo.
- 5.8. A Contratada deve assegurar à CAIXA, acesso a toda documentação comprobatória, em nome do provedor, que esclareça a Região/Zona de Disponibilidade escolhidos pela CAIXA para hospedagem de seus recursos.
- 5.9. A Contratada deve assegurar a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.
- 5.10. A Contratada deve garantir, em caso de decretação de regime de resolução da CAIXA pelo Banco Central do Brasil, acesso pleno e irrestrito aos contratos e acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados

e das informações, bem como aos códigos de acesso aos dados e às informações.

- 5.11. A Contratada deve garantir notificação prévia ao responsável pelo regime de resolução sobre a intenção da empresa Contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observado que:
- 5.12. A Contratada assegura o atendimento de eventual pedido de prazo adicional de (30) trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
- 5.13. Caso haja subcontratação do serviço em nuvem, desde que explicitamente autorizado pela CAIXA, é obrigatório a Contratada apresentar a garantia formal do atendimento das cláusulas deste item 3.2 por parte da Provedor de Serviços em Nuvem, seja por meio de declaração própria durante o processo de contratação, seja por meio de aditivo contratual, caso não previsto inicialmente no contrato original.

6. PROTEÇÃO DOS DADOS ARMAZENADOS EM NUVEM

- 6.1. Além dos requisitos descritos na seção 3, a Contratada também deve permitir trabalhar com chaves simétricas e assimétricas geradas e armazenadas pela CAIXA. Para tanto, ela deve prover meios que permitam o envio das chaves da CAIXA para o seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.
- 6.2. Caberá à CAIXA decidir quem fará a geração e a gestão de cada chave: se a própria CAIXA ou a Contratada.
- 6.3. Caso a CAIXA decida fazer a geração de chaves assimétricas, ela definirá a Autoridade Certificadora que será utilizada na emissão dos certificados digitais e fornecerá a cadeia certificadora para a Contratada sempre que necessário. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).
- 6.4. O modelo Third Party Certificates pode ser oferecido para o caso de certificados digitais utilizados no estabelecimento de conexões TLS. Nesse caso específico, as chaves devem ficar armazenadas exclusivamente em repositórios de chaves da Contratada e esta deve emitir o CSR (Certificate Signing Request) e enviá-lo para a CAIXA, que providenciará a emissão dos certificados digitais correspondentes. Após a instalação desses certificados,

todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).

- 6.5. Quando a Contratada for diferente do Provedor de Serviços em Nuvem e estiver agindo em nome deste, as chaves devem ser compartilhadas diretamente entre o Provedor e a CAIXA e a Contratada não deverá ter qualquer acesso às chaves envolvidas.
- 6.6. Quando se tratar de contratação no modelo IaaS, exige-se a certificação FIPS 140-2 nível 3.
- 6.7. Quando se tratar de contratação no modelo PaaS ou SaaS, exige-se a certificação FIPS 140-2 nível 2.
- 6.8. O Provedor de Serviços em Nuvem deve permitir que os usuários criptografem seus dados e objetos antes de enviá-los para o serviço de armazenamento.
- 6.9. A Contratada, assim como o Provedor de Serviços em Nuvem, deve tratar com rigor as informações sigilosas, não podendo ser usadas ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal da CAIXA.
- 6.10. A Contratada deverá assinar Termo de Confidencialidade resguardando que os recursos, dados e informações de propriedade da CAIXA, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.
- 6.11. Os dados, metadados, informações e conhecimento tratados pela Contratada, não poderão ser fornecidos a terceiros e/ou usados por esta para fins diversos do previsto, sob nenhuma hipótese, sem autorização formal da CAIXA.
- 6.12. A CAIXA e a Contratada obrigam-se por seus empregados, sócios, diretores e mandatários, manter total sigilo e confidencialidade no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ela relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

7. MONITORAÇÃO DOS DADOS TRATADOS EM NUVEM

- 7.1. A Contratada deverá fornecer, sempre que solicitado pela CAIXA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de APIs para análise de segurança e auditorias.

- 7.2. A trilha de auditoria deve conter, minimamente, itens descritos no item 2 deste documento.
- 7.3. O Provedor de Serviço em Nuvem, deve dispor de recurso que permita o gerenciamento centralizado de eventos e envio para a CAIXA, sempre que solicitado, de logs/informações de trilha.
- 7.4. Os registros do Provedor de Serviço em Nuvem deverão incluir ainda todos os acessos, incidentes e eventos cibernéticos, no ambiente do mesmo, pelo período 5 (cinco) anos.

8. SEGURANÇA DO TRÁFEGO DE DADOS COM A NUVEM

- 8.1. A comunicação entre a CAIXA e a Contratada deve suportar criptografia TLS, com autenticação mútua, na versão 1.3.
- 8.2. Caso a aplicação não suporte TLS 1.3, será admitida a compatibilidade para TLS 1.2.
- 8.3. A necessidade de TLS também se aplica a qualquer comunicação entre a Contratada e o Provedor de Serviços em Nuvem ou entre a CAIXA e o Provedor de Serviços em Nuvem, para todos os casos em que a Contratada e o Provedor forem entidades distintas.
- 8.4. O Provedor de Serviços em Nuvem deverá prover segurança relacionada ao tráfego de dados, provendo aplicações de firewall, IPS e CASB para garantir a segurança de todos os fluxos, sejam externos ou em trânsito com a CAIXA.
- 8.5. O Provedor de Serviços em Nuvem não deverá ter permissão de uso ou acesso direto ao ambiente de autenticação da CAIXA.
- 8.6. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, com pelo menos uma cópia atualizada de segurança também no Brasil.

9. OUTROS CONTROLES DE SEGURANÇA NO AMBIENTE DA CONTRATADA DO SERVIÇO DE NUVEM

- 9.1. O Provedor de Serviços em Nuvem deve habilitar o registro completo do Hypervisor que suporta os serviços da CAIXA, e deve suportar o uso de máquinas virtuais (Trusted VM) fornecidas pela CAIXA, desde que estas

máquinas estejam em conformidade com as políticas e práticas de segurança de rede exigidas pelo Provedor.

10. EVIDÊNCIAS DE CONFORMIDADE E PROCEDIMENTOS OPERACIONAIS PARA A FISCALIZAÇÃO DO FORNECEDOR

- 10.1. Com a existência de vários controles de segurança, muitos deles de caráter técnico, torna-se necessário que as áreas gestoras de Segurança da Informação, Segurança Cibernética, Arquitetura de TI e Risco de TI definam os procedimentos adequados de como realizar e registrar a fiscalização.
- 10.2. A seguir são definidas as formas de validação dos requisitos de segurança cibernética listados neste Guia e a etapa do ciclo de vida do fornecedor em que elas devem ser aplicadas. Trata-se de uma série de certificações reconhecidas no mercado, aplicáveis a fornecedores de solução em nuvem.
- 10.3. Para serviços de nuvem, caso a Contratada pela CAIXA e o Provedor de Serviços em Nuvem sejam empresas diferentes, a referida Contratada terá a responsabilidade de obter as documentações exigidas do Provedor, para apresentação à CAIXA.
- 10.4. Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo. O Due Diligence presencial é facultativo e será feito a critério da CAIXA.
- 10.5. Caso o prazo de validade da certificação ainda esteja vigente com relação à última apresentação, não é necessária uma nova apresentação.

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança do presente Guia	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada pela CAIXA	SOB DEMANDA

Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrição do Guia	<p>Conjunto de documentos listados na seção 5, combinados com qualquer outro que se faça necessário para comprovar atendimento dos requisitos do Guia.</p> <p>Quando não comprovados por certificação, os itens exigidos no Guia devem ser certificados por empresa de auditoria independente.</p>	<p>Relatórios próprios da empresa para comprovação do atendimento aos itens do Guia, desde que ratificados por empresa de auditoria independente</p> <p>Relatório de empresa de auditoria independente, a ser apresentado pela Contratada</p>	SOB DEMANDA
----------------------	---	--	---	-------------

10.6. CERTIFICAÇÕES APLICÁVEIS AOS FORNECEDORES DE SERVIÇOS EM NUVEM:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
FIPS 140-2 Nível 2 para SaaS e PaaS e FIPS 140-2 nível 3 para IaaS	Garantir que o provedor tenha mecanismo seguro para proteção de chaves criptográficas que sustentem os seus processos	Certificação do NIST que atesta um nível elevado de segurança para o HSM	Apresentar certificado FIPS 140-2 para equipamento utilizado no Provedor de Serviços em Nuvem	ANUAL

Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade, confidencialidade e privacidade	SOC TYPE 2 Fornece relatórios com descrição do ambiente de controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA	Disponibilizar relatório de auditoria em nome do Provedor de Nuvem	SEMESTRAL
----------------------------------	--	--	--	-----------

11. GLOSSÁRIO

- 11.1. AICPA (American Institute of Certified Public Accountants) - Instituto Americano de Contadores Públicos Certificados - É a associação profissional nacional dos contadores dos Estados Unidos, com mais de 330.000 membros, incluindo contadores com atuação em negócios, indústria, governo e educação, estudantes e associados estrangeiros.
- 11.2. Atividades críticas - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo (Adaptado da portaria PR/GSI nº 93, de 26 de setembro de 2019).
- 11.3. BYOD (Bring Your Own Device) – política que prevê a utilização de recursos do próprio empregado para realização das atividades laborais.
- 11.4. CASB (Cloud Access Security Broker) – Agente de segurança em nuvem que monitora as atividades e aplica políticas de segurança.
- 11.5. Dados estratégicos – dados que subsidiam a tomada de decisão, planos estratégicos, planejamentos, diretrizes, análise de riscos, oportunidades e ambições da CAIXA, podendo estar relacionados a processos e/ou produtos estratégicos/prioritários para a empresa. A perda, modificação ou divulgação não autorizada desses dados pode afetar a competitividade e a governança corporativa da CAIXA.

- 11.6. Fornecedor – pessoa física ou jurídica contratada para fornecer bens ou serviços para a CAIXA, o qual se encontra integrado à cadeia produtiva da empresa.
- 11.7. FIPS (Federal Information Processing Standards) – padrões desenvolvidos pelo NIST para uso em sistemas de computador por agências do governo americano não-militares e contratantes do governo.
- 11.8. Gestor de TI – empregado com atribuições gerenciais designado pela Unidade Executora para coordenar e comandar a utilização e execução no tocante aos aspectos técnicos do contrato, conforme TE165.
- 11.9. Hardening - é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- 11.10. HSM (Hardware Security Module) – equipamento para o armazenamento seguro de chaves criptográficas.
- 11.11. Informação Corporativa - informação não pública que possui valor para o negócio da CAIXA e sua perda, modificação ou divulgação não autorizada pode gerar impactos para a CAIXA.
- 11.12. Informação Pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem abrangendo clientes ou empregados da CAIXA.
- 11.13. Key Vault – Estrutura segura de armazenamento para chaves criptográficas e certificados.
- 11.14. LGPD – Lei Geral de Proteção de Dados, no 13.709 de 14 de agosto de 2018.
- 11.15. MAM (Mobile Application Management) – Solução que permite controlar os dados de negócios nos dispositivos pessoais dos usuários.
- 11.16. MDM (Mobile Device Management) – Solução que permite configurar políticas de proteção de dados em seus dispositivos móveis. Quando um dispositivo está sob o gerenciamento de dispositivo móvel, é possível controlar todo o dispositivo, apagar dados dele e também redefini-lo para as configurações de fábrica.
- 11.17. NAC (Network Access Control) – Tecnologia que viabiliza a implementação de políticas para controlar o acesso à rede corporativa. Tais políticas podem

ser baseadas em autenticação do dispositivo, configuração do endpoint (postura) ou identidade do usuário.

- 11.18. NIST (National Institute of Standards and Technology) – Instituto de padrões de tecnologia do governo dos Estados Unidos da América.
- 11.19. OTP (One Time Password) – Senha de uma única utilização.
- 11.20. OWASP (Open Web Application Security Project) – Fundação que orienta internacionalmente ações para melhoria da segurança de software.
- 11.21. Regime de Resolução - quando uma instituição financeira apresenta grave comprometimento do seu patrimônio ou dificuldade de honrar seus compromissos, o Banco Central (BC) pode determinar aos seus controladores que aportem os recursos necessários, transfiram o controle, reorganizem a sociedade ou adotem medidas de recuperação.
- 11.22. Relacionamento com Fornecedor – conjunto de ações realizadas previamente e durante a vigência dos contratos que favoreçam a gestão dos mesmos, mantendo-se um clima de parceria, sem prejuízo do acompanhamento do cumprimento das cláusulas contratuais.
- 11.23. Tratamento de Dados - toda operação realizada com dados pessoais ou corporativos, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- 11.24. SOC (Service Organization Controls) – Serviço de auditoria independente que avalia requisitos de conformidade e geração de relatórios.
- 11.25. SSO – Ferramenta de Single Sign-On

ANEXO I-C**SEGURANÇA DA INFORMAÇÃO****GRAU DE CRITICIDADE SEGURANÇA DA INFORMAÇÃO – Máximo****1. Cláusulas Gerais de Segurança da Informação:**

1.1 A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (<https://www.caixa.gov.br/Downloads/caixagovernanca/politica-seguranca-informacao.pdf>), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto do contrato.

1.2 A CONTRATADA deve proteger as informações corporativas da CAIXA e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.

1.3 A CONTRATADA deve garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações obtidas durante a prestação dos serviços ou em função deles e somente as utilizem no âmbito dos serviços contratados.

1.4 A CONTRATADA deve garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social.

1.5 A CONTRATADA deve garantir que as práticas de segurança da informação por ela executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento.

1.6 A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.

1.7 A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação.

1.8 A CONTRATADA fica ciente de que deve guardar o mais completo e absoluto SIGILO em relação às informações e dados que tiver conhecimento em razão do serviço a ser prestado, observadas as solicitações de órgãos de regulação, fiscalização, supervisão e de controle, bem como as determinações judiciais que deverão ser comunicadas imediatamente, pois ambas somente poderão ser atendidas mediante prévia autorização da área jurídica da CONTRATANTE.

1.9 A CONTRATADA fica ciente que, por força da lei, é responsável civil e criminalmente pela divulgação indevida, descuidada ou incorreta utilização das informações

corporativas da CAIXA e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.

1.10 A CONTRATADA deve comunicar imediatamente à CONTRATANTE qualquer descumprimento às cláusulas acima, principalmente para os casos em que ficar comprovado o comprometimento de informação corporativa da CAIXA ou sob sua responsabilidade.

2. Cláusulas Específicas de Segurança da Informação

2.1 A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, anexo.

2.2 A CONTRATADA deve enviar, anualmente, à CONTRATANTE a versão vigente do(s) Termo(s) de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, a ser disponibilizado pela área gestora do contrato, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).

2.3 A CONTRATADA deve realizar ou contratar, treinamento para seus dirigentes, empregados e colaboradores, visando a sensibilização e conscientização em relação à segurança da informação e privacidade de dados, abordando no mínimo 80% do seguinte conteúdo:

Grau de Criticidade em SI Alto ou Máximo		
Domínio Temático	Conteúdo	Carga Horária Anual
Política de Segurança da Informação	- Conhecimento da política de segurança da informação da empresa e da Política de Segurança e Informação da CAIXA	8 horas
Tratamento da Informação	- Uso seguro de informações corporativas a que tiver acesso; - Adoção da política de "mesa limpa", "tela limpa" e "impressora limpa"; - Descarte seguro de informação.	
Reporte de Incidentes	- Formas de reporte de incidentes de segurança da informação na empresa e na CAIXA	
Privacy by Design e Secure by Design	- Metodologia e princípios	
Fundamentos para Segurança Digital	- Conceitos básicos de segurança digital; - Uso da Internet	
Segurança de Dispositivos Digitais Pessoais	- Proteção e privacidade em dispositivos digitais pessoais; - Conhecimento, configurando e usando o dispositivo; - Mantendo o dispositivo;	

	- Vulnerabilidades e ameaças
Segurança em Redes	- Segurança na Internet; - Segurança em redes wi-fi públicas; - Proteção de redes pessoais; - Computação em nuvem
Segurança do Usuário	- Autenticação no acesso a sistema e a serviços; - Proteção de contas pessoais; - Mídias sociais; - Segurança com e-mails; - Armazenamento e compartilhamento de dados; - Qualidade de vida digital; - Segurança de dados do usuário em viagens
Segurança e Comportamento em Mídias Sociais	- Netiqueta; - Construindo seu perfil na Internet; - Segurança em mídias sociais; - Administrando seu rastro digital; - Uso saudável de mídias sociais; - Fake News; - Jogos online
Comunidades Digitais	- Educação na Internet; - Construindo comunidades digitais cidadãs; - Empreendedorismo na Internet
Criptografia	- Criptografia; - Certificação Digital; - Assinatura Digital
Direito Digital	- Conceitos jurídicos e legislação relacionada à segurança da informação; - Direitos autorais; - Fraudes; - Assédio virtual; - Crimes cibernéticos; - Crimes na Internet; - *Hacktivismo
Prevenção à fraude	- Engenharia social (formas defensivas contra **Phishing e ***Smishing)

2.3.1 O treinamento referido no item 2.3 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 08 horas.

2.4 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao ano base, a documentação comprobatória de cumprimento do treinamento referido no item 2.3.

2.5 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do período, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA.

2.6 A CONTRATADA deve se adequar às normas e a legislação vigente inerentes à Segurança da Informação relacionadas às atividades da CONTRATANTE, enquanto empresa pública e instituição financeira.

2.7 A CONTRATANTE poderá exercer o direito de exigir alterações nos controles de segurança da CONTRATADA, à medida que os ambientes externos e internos se modifiquem.

2.8 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores:

a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, treinados em SI, conforme item 2.3 no último ano dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base;

b) Quantidade de empregados que assinaram o Termo de Responsabilidade de Segurança da Informação, previsto no item 3.1, dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base;

2.9 O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente instrumento contratual, implicará em:

a) Multa de 0,25% do valor global do contrato por item até o limite de 1% do valor global.

b) Rescisão contratual em caso de impacto grave que gere prejuízos financeiros e/ou de imagem para a CAIXA

2.10 Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a comunicar a CAIXA e providenciar a solução tempestivamente.

2.11 Quaisquer materiais ou documentos com informações confidenciais que tenham sido fornecidos à CONTRATADA pela CONTRATANTE serão devolvidos, acompanhados de todas as cópias, em até 5 (cinco) dias, a partir da formalização de solicitação de devolução das informações confidenciais pela CONTRATANTE.

2.12 No encerramento/extinção do contrato a CONTRATADA se compromete a:

a) entregar todos documentos/manuais técnicos sob sua custódia;

b) executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CONTRATANTE ou a quem ela indicar, observada a regulamentação vigente;

c) devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.

d) Fornecer todo histórico de informações e vulnerabilidades sobre os ativos vinculados as licenças vigentes na data de encerramento.

3. Cláusulas Específicas de Segurança da Informação

3.1 A CONTRATADA é responsável por realizar o tratamento das informações da CAIXA e as sob sua responsabilidade, observando sua classificação de sigilo, bem como as demais regras internas da CAIXA estipuladas na versão vigente do manual normativo OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.

3.2 A CONTRATADA, durante a execução dos serviços contratados, deve adotar a mesma classificação da informação adotada pela CONTRATANTE, observar e cumprir as regras internas da CONTRATANTE quanto ao tratamento de informações sensíveis e confidenciais da CAIXA, previstas no OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.

3.3 A CONTRATADA é responsável pelas informações que obtiver, em razão de acesso aos recursos computacionais da CAIXA e se compromete a tomar conhecimento e cumprir as regras de uso aceitável e não aceitável da informação.

3.4 O treinamento de segurança da informação e proteção de dados referido no item 2.3 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 08 horas.

3.5 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento do treinamento referido no item 3.4 e, caso estabelecido pela CONTRATANTE.

3.6 A CONTRATADA deve emitir relatório, anualmente, até o último dia útil do mês subsequente ao término do ano base, relacionados aos seus riscos de segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CONTRATANTE.

3.7 O relatório referido no item anterior deve proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.

3.8 A CONTRATADA garantirá que a CONTRATANTE, ou a auditoria independente indicada pela CONTRATANTE, ou os órgãos de regulação/fiscalização das atividades de atuação da CAIXA tenham acesso físico e lógico ao seu ambiente e às informações relacionadas ao objeto do contrato, para realizar verificações relativas aos padrões de segurança da informação.

3.9 A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.

3.10 A CONTRATADA deve reportar imediatamente à CONTRATANTE os incidentes de segurança da informação identificados em seu ambiente ou operação e em toda sua cadeia produtiva.

3.11 A CONTRATADA deve enviar à CONTRATANTE, em até 05 dias úteis da detecção da ocorrência, relatório detalhado sobre o incidente de segurança da informação identificado, seus impactos, medidas corretivas implantadas e a implantar.

3.12 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores mencionados no item 2.10 e dos demais a seguir:

a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, que obtiveram nota mínima de aprovação no treinamento relacionado a Segurança da Informação mencionado no item 2.3 /Quantidade total de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;

b) Quantidade de relatórios, referidos no item 3.6, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;

c) Quantidade de relatórios, referidos no item 3.11, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base.

3.13 A CONTRATADA deve garantir a continuidade do processamento das informações críticas de negócios, no caso de contratação de bem ou serviço de suporte às atividades críticas da CAIXA.

3.14 A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos.

3.15 A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.

4. Cláusulas Específicas de Segurança da Informação

4.1 A CONTRATADA deve apresentar, sempre que requerido pela CONTRATANTE, relatórios emitidos por empresas de auditoria especializada independente que tenha realizado trabalho de auditoria em segurança da informação na CONTRATADA e

certificações que atestem o nível de confiança nos princípios de segurança da informação.

4.2 A CONTRATADA se responsabiliza pelos incidentes de segurança detectados em sua infraestrutura ou na infraestrutura de empresa subcontratada.

ANEXO I-D - HOMOLOGAÇÃO DA AMOSTRA**1. ANÁLISE DOCUMENTAL**

- 1.1. A documentação técnica para homologação da SOLUÇÃO deverá ser fornecida em até 10 (dez) dias corridos após a solicitação do pregoeiro.
- 1.2. A documentação técnica deverá ser indexada, ter apresentação gráfica de boa qualidade, conter a descrição detalhada de todas as funcionalidades da SOLUÇÃO, seu dimensionamento e ser fornecida em mídia digital.
- 1.3. A documentação técnica e os manuais dos produtos deverão ser da versão de produção dos produtos, redigidos em língua portuguesa (Brasil) ou excepcionalmente em língua inglesa.
- 1.4. A documentação técnica deverá conter arquivos específicos para cada componente da SOLUÇÃO (SIEM, SOAR, UEBA e demais componentes de gerenciamento e operação da solução).
- 1.5. As seguintes informações devem constar na documentação:
 - Fabricante: nome do fabricante dos componentes da solução ofertada;
 - Modelo: modelo dos componentes da solução ofertada;
 - Versão: versão dos componentes da solução ofertada;
 - Procedência: procedência dos componentes da solução ofertada – país de origem;
 - Fabricação: ano de fabricação dos componentes da SOLUÇÃO;
 - Suporte: endereço na Internet (site) do fabricante, onde seja possível a obtenção dos manuais técnicos (especificações detalhadas, FAQ, etc.) e drivers atualizados.
- 1.6. A documentação técnica deverá conter a arquitetura da SOLUÇÃO, contendo descrição lógica e física da solução proposta, dos seus dispositivos e das funcionalidades a serem implementadas nos mesmos.
- 1.7. O desenho de arquitetura deverá ser específico para este projeto, de acordo com as necessidades e o cenário solicitados neste edital.
- 1.8. Na descrição lógica deverão ser identificadas as funções de cada componente da solução proposta e os fluxos da informação (as entradas e saídas dos componentes).

- 1.9. Na descrição física deverão ser identificados os componentes físicos da solução proposta e os fluxos que conectam esses componentes entre si e com outros sistemas corporativos, modelando os detalhes contidos na SOLUÇÃO em termos de hardware e software.
- 1.10. Deverão ser fornecidos, junto com a documentação técnica, manuais que contenham informações suficientes para possibilitar a configuração, operação e conexão dos módulos da solução.
- 1.11. Deverão ser entregues os seguintes manuais. Se possível, em documentos distintos:
- Manual de configuração, com o detalhamento dos procedimentos adotados, incluindo scripts de configuração dos equipamentos e das funcionalidades, de forma a tornar operacional a solução;
 - Manual de operação e manutenção;
- 1.12. A documentação técnica de homologação deverá conter a relação dos softwares que compõem a solução.
- 1.13. A análise da documentação técnica será realizada com base nos requisitos técnicos e demais especificações contidas no ANEXO I – TERMO DE REFERÊNCIA e demais anexos que o complementam.
- 1.14. Para a análise da documentação técnica, deverá ser apresentada pela PROPONENTE planilha eletrônica consolidada com todos os itens da especificação técnica, com cópia editável, em formato “DOC”, “DOCX”, “XLS” ou “XLSX”, na forma do modelo abaixo:

ITENS	ANÁLISE	OBSERVAÇÃO	TÍTULO DO DOCUMENTO/ LINK WEB DE REFERÊNCIA
3.1.2	Atendido		
3.1.3	Atendido		

Tabela 01 – Modelo de tabela da documentação técnica

- 1.15. A ordem dos itens deverá obedecer a ordem contida na especificação técnica.

- 1.16. Na planilha, para a comprovação de cada item do edital, deverá ser referenciada a documentação oficial do fabricante (nome do documento e/ou link em página Web).

2. TESTE DE BANCADA:

- 2.1. A segunda fase da homologação da SOLUÇÃO será realizada em laboratório (ambiente de testes de bancada e homologação) o qual deverá conter uma amostra mínima da principais módulos da solução, conforme descrito no ANEXO I-E - CADERNO DE TESTES, ocasião em que deverão ser simuladas situações de alertas de incidentes cibernéticos correlacionados no SIEM de teste da PROPONENTE.
- 2.2. A PROPONENTE deverá disponibilizar ambiente de testes para homologação, capaz de demonstrar que a SOLUÇÃO proposta atende aos requisitos técnicos, em até 15 (quinze) dias corridos após a solicitação do pregoeiro.
- 2.3. No momento da apresentação da documentação técnica para a fase da homologação documental, será agendado junto a equipe técnica da CAIXA e a PROPONENTE reunião de alinhamento para organização dos testes em laboratório.
- 2.4. Os testes ocorrerão de forma remota, em sala no Microsoft TEAMS.
- 2.5. A PROPONENTE poderá indicar até 05 (cinco) profissionais da empresa PROPONENTE para demonstração e realização dos testes na ferramenta de SIEM.
- 2.6. A infraestrutura do teste deverá ser em ambiente fechado, na nuvem da PROPONENTE, exclusivo para os testes.
- 2.7. A PROPONENTE, poderá fazer uso de ambiente de simulação de ataques para sensibilização dos alertas do SIEM, caso seja necessário, também poderá fazer uso de ferramentas de gerenciamento de Tickets de incidentes para captura dos alertas gerados como incidentes.
- 2.8. A PROPONENTE também poderá fazer uso de scripts, automações ou equipe própria para realização dos ataques simulados que servirão para sensibilização do SIEM de teste.
- 2.9. Todo o ambiente de simulação para entrada, processamento e saída dos alertas gerados deverão ser demonstrados pela PROPONENTE no início dos testes.
- 2.10. Em nenhuma hipótese será utilizado qualquer infraestrutura cibernética da CAIXA para realização dos testes simulados, cabendo a PROPONENTE toda a criação do ambiente.

- 2.11. Os testes deverão ser executados no horário das 9h00 às 18h00, com pausa de duas horas de almoço, e terão duração máxima de cinco dias úteis, caso seja necessário.
- 2.12. O horário dos testes poderá ser flexibilizado, caso ocorram intercorrências por parte da CAIXA ou da PROPONENTE, sendo previamente ajustado e avisado para as demais licitantes que estejam acompanhando o processo.
- 2.13. A homologação da amostra em ambiente de laboratório se dará com base nos critérios definidos no ANEXO I-E - CADERNO DE TESTES devendo a PROPONENTE atendê-los integralmente.
- 2.14. A CAIXA poderá solicitar a realização de testes adicionais aos previstos no Cadernos de Testes, em virtude de particularidades da SOLUÇÃO proposta, referentes a quaisquer requisitos técnicos da SOLUÇÃO, constantes nas especificações técnicas deste edital.
- 2.15. Caso a PROPONENTE solicite ajustes no ambiente de homologação, ficará sujeita a repetição de todos os itens do Formulário de Homologação, sem prorrogação do período de homologação.
- 2.16. Devido à criticidade desta etapa, recomenda-se ao PROPONENTE a realização prévia de todos os testes a fim de evitar, nos dias da homologação, imprevistos que acarretem a extrapolação do prazo e, consequentemente, sua desclassificação.
- 2.17. Todos os testes deverão ser acompanhados por, no mínimo, 02 (dois) funcionários da CAIXA.
- 2.18. É permitida a participação das demais licitantes no acompanhamento do procedimento de avaliação da amostra somente como ouvintes e desde que não interfiram na realização dos testes.
- 2.19. Ao final de cada etapa do teste, será disponibilizado para as demais licitantes tempo para questionamentos sobre o item apresentado.
- 2.20. Para participação nos testes, será disponibilizada para as demais licitantes, sala de reunião em ambiente Microsoft TEAMS, para acompanhamento da apresentação a ser realizada pela PROPONENTE junto à equipe da CAIXA.
- 2.21. No final dos testes, os funcionários da CAIXA e os representantes da empresa PROPONENTE subscreverão o documento, representando a conclusão da etapa do processo de homologação do PROPONENTE.

ANEXO I-E - CADERNO DE TESTES**1. AMBIENTE DE LABORATÓRIO**

- 1.1. Para a realização dos testes de homologação da SOLUÇÃO, a PROPONENTE deverá demonstrar em ambiente de teste todas as funcionalidades citadas nas tabelas A, B, C.
- 1.2. ITEM - Avaliar as funcionalidades descritas na coluna FUNCIONALIDADE.
- 1.3. Procedimento: Apresentar o solicitado na coluna DESCRIÇÃO.
- 1.4. Resultado esperado: Para cada item apresentado, será aplicado a seguinte resposta:
Atendido () NÃO atendido ()

A - INTEGRAÇÃO E NAVEGAÇÃO

SUBITEM	FUNCIONALIDADE	DESCRIÇÃO
1.	Integração do <i>SIEM</i> com o <i>TheHive</i> para envio dos Incidentes/alertas	Demonstrar a integração do SIEM (<i>SaaS</i>) com a ferramenta de gestão de alertas/incidentes <i>TheHive Project</i> , para envio dos alertas/incidentes. https://github.com/TheHive-Project/TheHive
2.	<i>SIEM</i>	Apresentar o módulo de correlação dos eventos e criação dos alertas.
3.	<i>SOAR</i>	Apresentar o módulo de criação e orquestração das respostas automatizadas pelo <i>SOAR</i> .
4.	<i>UEBA</i>	Apresentar módulo de <i>UEBA</i> , demonstrando as funcionalidades para comportamento de usuários e dispositivos.
5.	Inteligência Artificial	Demonstrar módulo/função de Inteligência Artificial (IA).
6.	Conectores	Apresentar como a ferramenta faz para coletar os seguintes logs: Mainframe z/OS, Linux, Windows.
7.	Inteligência de ameaças	Demonstrar módulo de integração com rede de inteligência (Threat intelligence) com os feeds de ameaças.

TABELA - A**B – DETECÇÃO E RESPOSTA - SIEM**

SUBITEM	FUNCIONALIDADE	DESCRIÇÃO
1.	Detectar e gerar alerta para Atividade de Comando e Controle (C2) Suspeita	Detectar eventos de conexões de rede que indicam comunicação com servidores C2,

		utilizados para o controle remoto de dispositivos comprometidos.
2.	Detectar e gerar alerta para ataque Web	Detectar atividades anômalas em aplicativos web, como tentativas de exploração de vulnerabilidades em páginas web com pelo menos uma das seguintes técnicas: <i>SQL Injection, XSS, Protocol Attack, Command Injection, Remote File Inclusion Attack</i> .
3.	Detectar e gerar alerta para Movimento Lateral Suspeito	Identificar tentativas de exploração interna em que um atacante tenta mover-se entre diferentes sistemas ou segmentos de rede.
4.	Detectar e gerar alerta para uso de Ferramentas de Acesso Remoto Não Autorizadas	Detectar o uso de ferramentas como <i>AnyDesk, TeamViewer</i> ou outras não permitidas em ambiente corporativo.
5.	Detectar e gerar alerta para Ataque de força-bruta ou pulverização de senha (<i>Password Spray</i>)	Detectar múltiplas falhas de autenticação em curto período da mesma ou várias origens.
6.	Detectar e gerar alerta para atividades de varredura de portas de rede	Detectar múltiplas varreduras de portas de rede originadas de um mesmo Endereço IP.
7.	Detectar e gerar alerta para eventos de tunelamento de DNS	Detectar eventos de tunelamento DNS.
8.	Detectar e gerar alerta para eventos de tunelamento SSH	Detectar eventos de tunelamento SSH.
9.	Detectar e gerar alerta para eventos de ataques de força bruta em API	Detectar tentativas de autenticação em endpoints de API.
10.	Detectar e gerar alerta para eventos de uso de ferramentas de <i>Pentest</i>	Detectar eventos de uso de <i>Nmap, Metasploit, BloodHound, Mimikatz</i> , etc.
11.	Detectar e gerar alerta para eventos de escalção de privilégio	Detectar eventos de escalção de privilégio (Ex.: <i>Sticky Keys</i> ou outros métodos).
Observações: A PROPONENTE deverá apresentar adicionalmente, um caso prático com uso de UEBA e a aplicação de funcionalidades de Inteligência Artificial em pelo menos um dos casos de uso.		

TABELA - B

C – ORQUESTRAÇÃO DE RESPOSTAS - SOAR

SUBITEM	FUNCIONALIDADE	DESCRIÇÃO
1.	Executar isolamento de computador para alertas específicos	Isolar computador na rede quando forem gerados alertas específicos (Ex.: <i>Sticky Keys</i> ou outros métodos para escalação de privilégio).
2.	Enviar <i>Card</i> ou mensagem para usuários em aplicativo de comunicação instantânea	Enviar <i>Card</i> ou mensagem para usuários em aplicativo de comunicação instantânea.
3.	Executar fechamento automático de alerta/incidente falso-positivo	Identificar com base em análise automatizada falso-positivo e proceder fechamento automático do alerta/incidente.
4.	Executar ação automatizada para forçar a troca de senha ou bloqueio da conta do usuário	Executar ação automatizada para forçar a troca de senha ou bloqueio da conta do usuário em base de autenticação.
5.	Bloqueio de IP de origem	Demonstrar resposta automatizada para bloquear o IP de origem via integração com firewall.

TABELA - C**D – FUNCIONALIDADES ESPECÍFICAS**

SUBITEM	FUNCIONALIDADE	DESCRIÇÃO
1.	Capacidade de processamento e ingestão em picos de volume de logs	Simular a ingestão de eventos de pelo menos 100 mil eventos por segundo, durante 5 minutos, para avaliar a latência no processamento.
2.	Análise de violação de dados	Demonstrar um caso de violação de dados (ex.: exfiltração de arquivos sensíveis) com rastreamento completo da cadeia de eventos, com uso de recurso de <i>timeline</i> para visualização das informações, incluindo origem, usuário envolvido e destino dos dados.
3.	Geração de relatórios	Demonstrar a geração de relatórios customizados, permitindo a seleção de campos, período e filtro. Ex.: Relatório de incidentes, ocorridos no último mês, para severidade média e alta, contendo nome do incidente, data de ocorrência, entidades envolvidas, severidade,

		<i>MTTA(Mean Time to Acknowledge), MTTC (Mean Time to Conclusion).</i>
4.	Técnicas de processamento de linguagem natural (PLN)	Demonstrar a utilização de técnicas de processamento de linguagem natural (PLN): Gerar resumo executivo de determinado incidente, gerar código de pesquisa para execução de busca avançada de determinados eventos específicos, ex.: Gerar uma consulta para eventos de segurança das últimas 2 horas com falhas de autenticação, severidade alta, originadas da rede interna/local, contendo padrão de tentativas de <i>brute force</i> .

TABELA - D

ANEXO I-F CONEXÃO COM A CAIXA

1. O acesso padrão para conexão com a Rede Caixa (conexão entre a CONTRATADA e a CAIXA) é mediante o uso de circuito privado dedicado nas tecnologias LAN-to-LAN ou MPLS.
2. A instalação do circuito dedicado deve ser direcionada para o Centro Tecnológico Datacenter – DTC e/ou Centro Tecnológico CAIXA – CTC, de acordo com a indicação da equipe de Rede de Telecomunicações.
3. Os endereços de instalação são:

Parque Tecnológico Capital Digital Lote 03 – S/N
Bairro: Granja do Torto
Cidade: Brasília – DF
CEP: 70.636-000

Setor de Indústrias Gráficas – SIG Quadra 1 – Lote 685/705
Bairro: SIG
Cidade: Brasília – DF
CEP: 70.610-410

4. Nos casos em que o ambiente da CONTRATADA esteja hospedado em ambiente de nuvem ou nos Datacenters de interconexão Multicloud da Caixa em São Paulo ou Rio de Janeiro, as conexões poderão ser feitas através do FABRIC desses Datacenters.
5. Os endereços de instalação são:

Equinix SP IBX SP3
Av. Marcos Penteado de Ulhoa Rodrigues, 249
Santana de Parnaíba – SP
CEP: 06543-001

Equinix RJ IBX RJ2
Estrada Adhemar Bebian, 1380
Del Castilho – RJ
CEP: 21051-070

6. O circuito WAN de contingência deve ser instalado em localidade e operadora de telecomunicações diferente do circuito principal.
7. Caso a CONTRATADA disponha de duas ou mais localidades de processamento deve-se considerar a contratação de circuitos para todas essas localidades direcionados aos Datacenters da CAIXA.
8. A Caixa poderá alterar seus endereços de conexão, inclusive de cidade e/ou de estado, de acordo com as suas necessidades, o que deverá ser atendido sem ônus para a Caixa.
9. Características gerais da conexão:
 - a) O dimensionamento do link de comunicação é de responsabilidade da contratada.
 - b) A responsabilidade de fornecimento e negociação junto à operadora do roteador CPE na ponta da CONTRATADA é de inteira responsabilidade da CONTRATADA.
 - c) A operadora deverá fornecer, caso ainda não tenha, concentrador na ponta da CAIXA conforme padrões estabelecidos. Caso a operadora já disponha de infraestrutura e equipamentos nos SITE DA CAIXA, ou pretenda utilizar o FABRIC dos ambientes de Multicloud, esta deverá fazer uso compartilhado destes equipamentos/conexões.
 - d) A operadora deve adotar arquitetura de compartilhamento de conexões físicas, ou seja, não será autorizado o uso de conexões físicas exclusivas. Este compartilhamento deve ser observado na conexão entre o equipamento da operadora e da Caixa garantindo ativação de diversas conexões lógicas na mesma interface física.
 - e) Nova conexão física independente poderá ser solicitada pela Caixa caso a conexão atender a ambientes internos segregados, tais como ambiente de desenvolvimento ou homologação.
 - f) A conexão com os equipamentos da Caixa deverá ser feita através de interface ethernet (mínimo gigabitethernet).
 - g) O endereçamento IP para trânsito WAN e de serviço (range para hosts) serão definidos pela CAIXA.
 - h) As conexões devem possibilitar a ativação de roteamento dinâmico baseado em BGP (Border Gateway Protocol).
 - i) Não é permitida a instalação de equipamentos da CONTRATADA no ambiente da Caixa.
 - j) É admitida a instalação de equipamentos de operadora instalados para uso na modalidade compartilhada, exceto nos ambientes de Multicloud.
 - k) Caso a CONTRATADA já disponha de conexão com a Caixa para o mesmo ambiente deste contrato, a mesma poderá fazer uso desta desde que efetue o upgrade correspondente ao novo serviço e atenda aos padrões definidos nesta especificação.

10. Permite-se conexão para ambientes de DESENVOLVIMENTO/HOMOLOGAÇÃO por VPN IPSEC, via Internet, conforme abaixo:

- a) VPN site-to-site via Internet.
- b) O acesso à Internet da empresa deverá possuir IP Fixo.
- c) O dimensionamento deste acesso é responsabilidade da Empresa.
- d) A CONTRATADA deverá dispor de roteador e concentrador VPN sob sua inteira responsabilidade.
- e) A CAIXA fornecerá as definições de padrões para estabelecimento da VPN, porém não proverá suporte e manutenção na ponta da CONTRATADA.
- f) Deverá utilizar no mínimo protocolo IPSEC 3DES-SHA1 IKE com 112bits.