1. FINALIDADE

As informações contidas neste Anexo descrevem os requisitos gerais, quantitativos e características técnicas para contratação de ferramentas e serviços especializados de monitoração de ativos de rede e de segurança da informação, através de um Centro de Operações de Segurança (SOC). O projeto inclui o fornecimento de ferramenta de coleta e correlação de logs e eventos de segurança (SIEM), integrada a serviços de inteligência de ameaças (*Threat Intelligence Feeds*), serviços de SOAR (*Security Orchestration, Automation, and Response*), além de um módulo de gestão de operações e de resposta a incidentes de segurança da informação.

Os requisitos para fornecimento dos componentes especificados neste documento têm caráter obrigatório, devendo ser rigorosamente atendidos pelo LICITANTE/CONTRATADO. O não atendimento a qualquer das exigências desclassifica a proposta do LICITANTE. A comprovação de todos os requisitos deve ser feita através de documentos públicos que possam ser obtidos no sítio oficial de cada fabricante.

2. REQUISITOS TÉCNICOS

2.1 FERRAMENTA DE COLETA E CORRELAÇÃO DE EVENTOS DE SEGURANÇA (SIEM) – (ITEM 1)
LICENCIAMENTO E ARQUITETURA
• Deve ser fornecida ferramenta de coleta e correlação de eventos de segurança da informação. As licenças de uso da solução deverão ser na modalidade subscrição, o CONTRATADO deverá fornecer: o registro das licenças do *software* ou chaves de instalação, certificados de autenticidade e documentação técnica original do fabricante; o nome específico do produto, a versão, a categoria e o código de identificação unívoca do *software*; disponibilizar acesso a portal do fabricante, que permita a verificação da situação das licenças de *software*; suporte e garantia junto ao fabricante pelo período estabelecido no contrato.
• A garantia da solução ofertada deve permitir a atualização de versões de *software* durante a vigência do contrato e suas prorrogações, contados a partir da assinatura do contrato.
• A solução de SIEM deve ser fornecida em modelo SaaS, de forma que o fabricante seja responsável pela infraestrutura cloud que compõe a plataforma ofertada, não sendo permitido o fornecimento de soluções implementadas sobre infraestruturas de nuvem pública (IaaS) de terceiros ou própria do fornecedor;

• A solução deverá segregar logicamente os logs do BNB dos demais logs de outras empresas que utilizem a solução de SIEM SaaS na nuvem do fabricante;
• A solução deve ser monitorada para garantir disponibilidade e infraestrutura em tempo integral, 24 horas por dia, 7 dias por semana, durante todo o período de vigência do contrato;
• A solução deverá ter disponibilidade mensal mínima de 99,7%, conforme Nível Mínimo de Serviço (Anexo IV);
• O CONTRATADO deve entregar todas as licenças de software necessárias, atendendo durante toda a vigência do Contrato as especificações recomendadas pelo fabricante, considerando o cenário de utilização de todo o volume de licenças previsto no Contrato.
• A solução deve ser licenciada para atender, no mínimo, 16.000 (dezesseis mil) Eventos Por Segundo (EPS), para coleta, processamento, armazenamento e correlacionamento dos eventos, de forma sustentada.
• A solução deve permitir a recepção de eventos que excedam temporariamente os limites contratados, processando o volume excedente assim que volume for normalizado, mantendo a operação com situações de picos temporários, sem incorrer na perda de eventos e sem incorrer em qualquer cobrança adicional por excesso ou bloqueio da solução.
• A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de referência (*network appliance* ou virtualização), dimensionada para o *throughput* contratado de 16.000 EPS, desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos do BNB.
• Todos os módulos e componentes da solução devem ser fornecidos por um único fabricante, para garantir suporte completo em relação a funcionalidades, integrações e compatibilidade de 100% com a solução;
• Todos os módulos e componentes que compõem a solução deverão se integrar de forma nativa, visando constituir um ambiente homogêneo de monitoração, análise, investigação, inteligência, defesa cibernética e resposta a incidentes;
• Todos os módulos e componentes desta Especificação Técnica devem vir com a última versão de *software* disponível no momento da aquisição;
• Os recursos de SOAR, SIEM, *Threat Intell*, UEBA e *Machine Learning* devem ser concentrados em uma única console e possuir integração nativa;
• A solução deverá ser dimensionada para suportar o armazenamento de eventos de segurança em banco de dados dedicado, disponibilizando acesso aos logs de forma online via interface web por, no mínimo, 3 meses *hot storage* e 9 meses *cold storage* na NUVEM do FABRICANTE.
• A solução deverá possuir procedimento de envio dos dados para um sistema de armazenamento de longo prazo (*storage*) físico da CONTRATANTE, de forma comprimida, para que sejam arquivados e/ou recuperados após o período mínimo de armazenamento estabelecido na Nuvem do FABRICANTE;

• A solução deverá realizar o armazenamento dos logs de preferência em território brasileiro, caso não seja possível, poderá armazenar ou processar os logs fora do Brasil desde que atenda os seguintes pontos referentes aos serviços a serem prestados no exterior: o A CONTRATADA deve assegurar que a prestação dos serviços não causará prejuízos ao regular funcionamento do Banco; o A CONTRATADA deve informar ao Banco os países e as regiões em cada país onde os serviços serão prestados e os dados serão armazenados, processados e gerenciados, facultando ao Banco o aceite dessa localização; o A CONTRATADA deve prever alternativas para continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção de contrato de prestação de serviços; o A CONTRATADA deve assegurar, documentalmente, que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impeçam o acesso aos dados e às informações.
• A solução deve implementar comunicação criptografada entre os componentes envolvidos;
• A solução deve suportar a consolidação dos coletores de logs de localidades remotas em um concentrador central;
• A solução deve ter a capacidade de utilizar contas de usuários do AD interno do Banco para autenticação na console de gerenciamento, através de integração com o Microsoft Entra ID ou via SAML;
• A solução deve estar licenciada e permitir o uso de duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução. Caso a solução necessite de mais de uma console de gerenciamento, todas devem estar licenciadas e permitir o uso do MFA;
• A solução deve correlacionar os alertas com táticas e técnicas do MITRE ATT&CK.
CONSOLE DE GERENCIAMENTO
• A solução deve ser capaz de integrar em uma única console de visualização, todos os dados de logs coletados;
• A solução deve oferecer uma administração centralizada que permita realizar investigações, gestão de incidentes, gestão de alertas e gestão de relatórios;
• A solução deve ser baseada em plataforma WEB, com acesso via *browser* padrão de mercado, utilizando comunicação criptografada (HTTPS/TLS, versão 1.2 ou superior);
• A solução deve permitir a criação de perfis de visualização dos eventos derivados dos dados coletados;
• A solução deve possuir controle de acesso baseado em papéis e perfis de usuários;
• A solução deve controlar o acesso através de perfis permitindo acesso às funções de Administração, Incidentes, Configuração de Regras, atividades de Redes e Logs.
• A solução deve permitir a customização de perfis de visualização de eventos de acordo com o objetivo da investigação;
• A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas na console de gerência e investigação;

• A solução deverá possuir um *dashboard* integrado, com os seguintes recursos mínimos: o Disponibilizar *dashboard* contendo visão consolidada das métricas de segurança, para todos os ativos monitorados; o Possibilitar a customização do *dashboard*, adicionando relatórios e métricas; o Efetuar a análise dos eventos de segurança da informação em tempo real; o Possibilitar a análise por *drill-down*, permitindo detalhá-la a partir de um gráfico geral, descendo aos níveis da análise conforme necessidade;
• A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
• A solução deve permitir identificar a data e hora do último login, de forma a garantir que a credencial não esteja sendo compartilhada;
• A solução deve permitir a pesquisa de eventos em Alertas, Incidentes ou Listas.
• A solução deve interagir com o profissional de segurança através de interface de conversação que utilize inteligência artificial generativa. Ex.: ChatGPT, Microsoft Copilot, Meta AI, etc.
• A solução deve executar triagem de incidentes, investigação e remediação através de interface de conversação que utilize inteligência artificial generativa.
• A solução deve permitir realizar consultas através de interface de conversação que utilize inteligência artificial generativa.
• A solução deve suportar o recebimento de informações do tipo *hash*, IP, nome de domínio, nome de host e nome de usuários para uso em relatórios e dashboards.
GESTÃO DE OPERAÇÕES DE SEGURANÇA
• A solução deve possuir modulo de GESTÃO DE OPERAÇÕES DE SEGURANÇA, para investigação e tratamento de alertas, eventos e incidentes;
• A solução de SIEM deve registrar os alertas e incidentes no modulo de GESTÃO DE OPERAÇÕES DE SEGURANÇA, de forma automática, sempre que detectar um potencial incidente de segurança;

• A solução deverá estar atualizada e possibilitar acesso às principais funcionalidades, como: o *Dashboards*; o Integração com analistas do SOC; o Detalhes de eventos; o Ferramentas de investigação; o Gerenciamento de *tickets* e alertas; o Relatórios; o Orquestração de trabalho coordenado em etapas manuais e automatizadas;
• A solução deverá permitir o acesso, sem limitar o número de usuários simultâneos, desde que dentro da quantidade de usuários licenciados, a distintos painéis de controle, os quais deverão ser totalmente customizáveis, sem a necessidade do uso de programação, através da utilização de perfis diferenciados. Dentre os perfis disponíveis, a plataforma deverá, no mínimo, contemplar os seguintes dashboards/perfis específicos: o Operador Nível 1 - Responsável pela triagem inicial dos eventos; o Especialista Nível 2 - Responsável pela análise mais detalhada dos eventos e resolução de tickets; o Coordenador do SOC - Coordenador da equipe de analistas de Nível 1; o Coordenador dos especialistas – Coordenador da equipe de especialistas de Nível 2; o Auditoria – Responsável por auditoria interna ou externa;
• A solução deverá permitir a definição de times de analistas;

- A solução deverá permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:
    - Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
    - Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
    - Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros e atualização de campos;
    - Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
    - Definição das tarefas a serem executadas. A ferramenta deverá conter uma biblioteca de procedimentos de resposta já existente;
    - Permitir inserir comentários dos analistas no incidente, de forma a possibilitar o registro de todas as atividades de análise;
    - Permitir inserir análise forense de *host* e rede como um complemento da análise do incidente;
    - Permitir inserir análise de impacto relativo a Confidencialidade, Integridade e Disponibilidade;
    - Permitir registrar os resultados de um incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- A solução deverá permitir o recebimento de Alertas de Segurança com as seguintes características:
    - Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;
    - Dados de origem e destino, portas de origem e destino, domínios de origem e destino, endereço MAC de origem e destino, além de informações de contexto de negócios de cada dispositivo (de origem ou destino). As informações de contexto deverão incluir endereço IP, nome do dispositivo, tipo, unidade de negócios, site, índice de criticidade e conformidade, além do proprietário, tanto para os dispositivos de origem quanto dispositivos de destino. É necessário também incluir informações de localização do dispositivo, incluindo cidade, país e geolocalização tanto dos dispositivos de origem quanto dos dispositivos de destino dos alertas;
    - Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas;

• A solução deverá permitir a criação de Investigações de Incidentes que não sejam necessariamente relacionados à Segurança da Informação, que permitam o atendimento às seguintes características: o Data de criação, status, prioridade, dias em aberto, tipo de investigação (exemplo: *hacking*, má conduta, violação de ética, etc), identificação de confidencialidade, datas de início e término da investigação, título, sumário, analista atribuído, nome do solicitante, fonte, tipo de requisição, nível de urgência; o Definição do time de investigadores (proprietário, coordenador, gestor, funcionário de RH, responsável por Compliance, departamento jurídico. Inclusão de documentação através de arquivos anexos e eventuais conexões com Incidentes de Segurança já existentes; o Possibilidade de inclusão de comentários de atividades por parte dos analistas, permitindo desta forma a identificação clara de todo o processo investigativo; o Definição de procedimentos investigativos. A ferramenta deverá conter uma biblioteca de procedimentos investigativos já existente; o Permitir inserir informações de impacto ao negócio incluindo: impacto geral ao negócio, tipo de perda de negócio, rating de perda para o negócio, unidades de negócio afetadas, além de permitir a inclusão de riscos identificados; o Permitir inserir análise de impacto relativo à Confidencialidade, Integridade e Disponibilidade;
• A solução deverá permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
• A solução deverá possibilitar o registro de Análise Forense, tanto para rede quanto para host.
• A solução deverá permitir a inclusão de novos procedimentos de Resposta à Incidentes;
• A solução deve possuir recursos para criação de *playbooks* e scripts com foco em conformidade, auditorias, controles internos e demais áreas correlacionadas com *cybersecurity*;
• A solução deverá possibilitar a documentação de Brechas de Segurança;
• A solução deverá permitir que cada incidente a ser tratado pode possuir um responsável (dono), que pode alocar outras pessoas como responsáveis por cada uma das tarefas do incidente. Um coordenador poderá designar um incidente ou tarefa previamente alocada, para outro analista (ex, mudança de turno do SOC);
• A solução deve permitir a criação de SLAs, avaliando através de critérios objetivos o tempo de resolução de incidentes de maneira individualizada;
• A solução deve permitir o envio de *e-mails* ou notificações para os analistas quando houver mudança no status do chamado e/ou designação de chamado;
• A solução deve permitir a documentação dos incidentes de maneira manual ou automática de pessoas envolvidas no incidente, tarefas executadas, evidências e anotações;
• A solução deve permitir aos analistas conduzir investigações conjuntas, executando comandos e documentação automatizada do contexto do incidente;

• A solução deve realizar o pré-processamento de chamados para conectar incidentes novos com incidentes antigos;
• A solução deverá permitir a rastreabilidade das operações realizadas, referente à ação de *tickets* e em configurações;
• A solução deverá manter o histórico de todas as atividades realizadas pelos usuários, tais como criação de registro e atualizações de campos, vinculando o usuário que realizou cada procedimento;
• A solução deverá permitir a consulta e exportação das trilhas de auditoria, logs e históricos;
• A solução deverá prover mecanismo de proteção contra alteração e remoção indevida dos registros de auditoria;
• A solução deverá permitir atrelar os controles de segurança a incidentes efetivos e inefetivos;
• A solução deverá possibilitar a criação de políticas de SOC com a definição de proprietário e descrição dos detalhes, além da definição das partes interessadas;
• A solução deverá permitir a definição de contatos que inclua detalhes de endereço, telefones, localização, bem como informações sobre conhecimentos técnicos e formação;
• A solução deverá permitir a integração com sistemas externos de tratamento de chamados. Para isto, a plataforma deverá suportar integração com sistemas de terceiros via arquivos texto (CSV, XML), Banco de Dados, API via *Web Services* e REST, ou notificação via e-mail estruturado;
• A solução deverá ter estrutura de biblioteca baseada no NIST ou MITRE ATT&CK, permitindo o mapeamento direto para políticas, táticas, técnicas e controles de segurança;
• A solução deverá possuir uma base de dados de procedimentos de resposta à incidentes com, no mínimo, 10 procedimentos pré-existentes;
• A solução deverá permitir que novos procedimentos sejam incluídos na biblioteca interna;
• A solução deverá permitir a portabilidade dos dados, base de incidentes, base de conhecimento e logica dos processos definidos, podendo ser entregue em formatos: Base de Dados, arquivos texto (exemplo: CSV, XML, TSV e etc.) ou PDF.
SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)
• A solução deve possuir modulo de *Security Orchestration, Automation, and Response* (SOAR) combinando resposta a incidentes, orquestração e automação, além de recursos de gerenciamento de inteligência de ameaças (TI);
• A solução deve permitir integração nativa com a ferramenta de SIEM ofertada;
• A solução deve permitir a integração com soluções de controle de acesso à rede (NAC), permitindo a troca contínua de informações de identidade e contexto de rede;
• A solução deve permitir a integração com a ferramenta de proteção de *endpoint* utilizada pelo BNB para respostas automatizadas;
• A solução deve suportar integração com mecanismos DLP (*Data Loss Prevention*) para evitar exfiltração ou vazamento de dados confidenciais de *endpoints*;

• A solução deve permitir a integração com soluções de segurança de rede (*firewalls*) de, no mínimo, os seguintes fabricantes: o Palo Alto; o Fortinet; o Forcepoint; o Check Point; o Cisco.
• A solução deve suportar integração com ferramentas forenses digitais para análise avançada e coleta de evidências;
• A solução deve possuir capacidade de se integrar com ferramentas de terceiros através de API;
• A solução deve permitir integração com sistemas de análise de vulnerabilidades de, no mínimo, os seguintes fabricantes: o Qualys; o Tenable; o Rapid7.
• A solução deve listar as ferramentas ou integrações nativas disponíveis para avaliação e correção de vulnerabilidades;
• A solução deve possibilitar o gerenciamento de IP, nome de *host* e URL para detecções de regras, incluindo a criação e atualização de regras de detecção com base nesses indicadores;
• A solução deve disponibilizar integração a sistemas de gerenciamento de *tickets* para criação automática de *tickets*, incluindo a capacidade de personalizar as regras de criação de *tickets* e integração de fluxo de trabalho;
• A solução deve suportar integração com ferramentas de gerenciamento de serviços de segurança e outros produtos internos para resposta simplificada a incidentes e fluxos de trabalho de emissão de *tickets*;
• A solução deve possibilitar a definição e customização de ações de fluxo de trabalho para adequar processos e respostas a necessidades específicas;
• A solução deve possuir *playbooks* ou fluxogramas básicos pré-carregados os quais podem ser usados como modelos para desenvolvimentos posteriores;
• A solução deve possuir interface gráfica de criação e manutenção dos *playbooks* em forma de fluxograma, onde seja possível estabelecer a sequência das ações sem a necessidade de codificação;
• A solução deve possuir execução automática dos *playbooks* assim que identificada a presença de um evento ou execução através de ação manual;
• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de sanitização, ou correção de *misconfiguration*, com base em regras e políticas predefinidas;
• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de resposta a incidentes com base em regras e políticas predefinidas;

• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de investigação a incidentes com base em regras e políticas predefinidas;
• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de mitigação a incidentes com base em regras e políticas predefinidas;
• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de mitigação a incidentes com base em regras e políticas predefinidas;
• A solução deve suportar etapas personalizadas e/ou manuais em fluxos de trabalho (*playbooks*) para automatizar processos de restauração a incidentes com base em regras e políticas predefinidas;
• A solução deve possuir a capacidade de programação das tarefas de automação podendo agrupá-las em fluxogramas que representam uma ou mais atividades macro;
• A solução deve permitir que a programação possa utilizar o sequenciamento condicional onde uma execução de uma tarefa esteja relacionada com o status da execução do passo anterior;
• A solução deve possuir ambiente para depurar a sequência de automação sendo capaz de visualizar a execução em tempo real dos passos do fluxograma;
• A solução deve possuir um ambiente de simulação, como "*SandBox*", onde seja possível realizar teste de fluxogramas antes de utilizar em um ambiente de produção;
• A solução deve permitir aos analistas conduzir investigações conjuntas, executando comandos e documentação automatizada do contexto do incidente;
• A solução deve identificar incidentes relacionados utilizando parâmetros como IOC (indicadores de comprometimento) e conteúdo dos campos dos incidentes;
• A solução deve executar fluxogramas automatizados de ações com base em indicadores (IOC);
CARACTERÍSTICAS GERAIS
• Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM;
• A solução deve permitir a coleta de *logs* de forma distribuída e permitir a análise centralizada;
• A solução deve coletar e armazenar *logs*/eventos dos dispositivos;
• A solução deve ser capaz de coletar os *logs* dos ativos de rede e dos dispositivos de segurança de forma não intrusiva, sem a necessidade de instalação de agentes nos servidores do Banco;
• A solução deve possuir capacidade de coletar e correlacionar *logs* de sistemas operacionais Windows, Linux, Unix e AIX;
• A solução deve possuir capacidade de coletar e correlacionar *logs* de IBM z/OS de forma nativa ou com uso de agente externo (RACF, ACF2, Top Secret, DB2, CICS, dentre outros);

• A solução deve ser capaz de coletar e correlacionar *logs* de diversos tipos de dispositivos e soluções, tais como: firewalls, EDR, IPS, WAF, DLP, CASB, O365, proxies, servidores web, servidores DNS, *load balancers*, roteadores, *switches*, aceleradores WAN e demais dispositivos de rede;
• A solução deve ser capaz de coletar *logs* e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SSH, Microsoft Windows *Remote Management*, Microsoft Windows *Event Logging* API, *Network flow*, arquivos de *logs* recebido via FTP, arquivos de *logs* formatados por delimitadores, ODBC/JDBC e CISCO;
• A solução não deve exigir a adição de agentes ou *software* nos dispositivos monitorados, exceto quando o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de *logs* citado no item anterior;
• A solução deve suportar nativamente o recebimento de informações de pacotes de rede (*Flow*) coletados por ferramentas de terceiros, sendo capaz de analisar e correlacionar de forma contínua os dados recebidos;
• A solução deve ser capaz de coletar e armazenar todos os *logs* de ativos de rede e dos dispositivos de segurança, gravando-os em formato original para posterior uso em análises forenses;
• A solução deve armazenar os dados de registro reais, ou *RAW*, em um formato forense sem modificação, independentemente de outros recursos habilitados na solução, garantindo a integridade e a conformidade com os requisitos legais e regulamentares;
• A solução deve ter a habilidade de receber *logs*/eventos oriundos de um *relay* de syslogs;
• A solução deve permitir coleta de dados de fontes que não sejam de log, como bancos de dados de ativos ou soluções de gerenciamento de vulnerabilidades, correlacioná-los com dados de *log* e usar esse contexto adicional para tomar decisões de alerta, como alertar ou desativar um alerta;
• A solução deve suportar o recebimento de eventos no formato *Common Event Format* (CEF);
• A solução deve permitir o processamento de informações estruturadas de ameaças STIX™ (“*Structured Threat Information eXpression*”);
• A solução deve suportar a criação de interpretadores (*parsers*) para a integração de *logs* não suportados nativamente;
• A solução deve suportar a criação de interpretadores (*parsers*) customizados para no mínimo 20 sistemas proprietários, a serem definidos pelo CONTRATANTE;
• A solução deve possuir a capacidade de integração com outras soluções de segurança, por meio de envio de *logs*/eventos via protocolo SYSLOG;
• A solução deve utilizar formatos de *logs*/eventos nativos de cada fabricante dos dispositivos de segurança, sem utilizar um tipo de formato exclusivo e restrito, definido pelo fabricante da Solução de SIEM;
• A solução deve normalizar todos os *logs* recebidos de ativos de diferentes fornecedores, num formato comum;
• A solução deve suportar de forma nativa os *logs* de pelo menos 200 dispositivos diferentes de fabricantes variados;
• A solução ofertada deve permitir a correlação de eventos provenientes de *logs*;
• A solução deve consolidar eventos de log de dispositivos, terminais e aplicativos distribuídos;
• A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados coletados;

• A solução deve permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
• A solução deve possuir um ambiente de construção de regras que ofereça um mecanismo de testes (*debug*), visando a redução de erros de lógica e sintaxe;
• A solução deve permitir testar as regras de correlação em eventos passados, com um período de tempo e escopo claramente definidos;
• A solução deve realizar correlação histórica, fornecendo a opção de escolher o período a ser analisado, com suporte mínimo para correlação de 1 (um) a 7 (sete) dias, porém deve possibilitar a realização de *queries*, relatórios ou dashboards para um período superior de até 6 (seis) meses.
• As regras de correlação histórica devem processar logs e *flows*, gerando alertas quando os eventos/flows analisados corresponderem às especificações definidas na regra;
• A solução deve possuir, no mínimo, 100 regras de correlação especializadas na detecção de incidentes de segurança, produzidas, suportadas e atualizadas pelo fabricante da solução ou pela contratada;
• Dentre as regras de correlação fornecidas e suportadas pelo fabricante, deve possuir regras que, a partir dos diversos tipos de *logs* e *flows*, cubram os seguintes Casos de Uso: o Exfiltração de dados; o Identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados) ou GDPR (*General Data Protection Regulation*); o Suportar a integração com solução de análise de vulnerabilidade para a geração de incidente/alerta quando o alvo de um ataque é vulnerável ao ataque efetuado; o Comunicação de dispositivos internos com sites conhecidos por serem controladores de *botnet*. Caso a solução não entregue as regras pré-formatadas, devem ser contemplados serviços através da estrutura do fabricante ou do CONTRATADO para a criação destes casos de uso;
• A solução deve ser capaz de criar regras de detecção com base na combinação de logs com parâmetros adicionados ao contexto de fontes externas (por exemplo, sistema operacional, vulnerabilidades);
• A solução deverá associar, dinamicamente, usuários e suas localizações, com os seguintes recursos mínimos: o Endereço de IP ao nome do computador; o Endereço MAC; o *Switch* VLAN id; o Identificação do usuário logado.
• A solução deve ser capaz de criar regras de detecção baseadas na combinação de logs com parâmetros adicionados ao contexto de fontes de dados criadas dentro da solução, como atribuições de sub-redes a locais;

• A solução deve possuir capacidade de criar regras de correlação personalizadas que podem detectar ataques retroativamente;
• A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (*watchlist*), permitindo também a criação e edição automatizada e manual de listas.
• A solução deverá gerar alertas baseados no recebimento de logs dos ativos monitorados, pelo menos, das seguintes ameaças: o *Host scans, port scans, scans* negados, repentino aumento ou redução do tráfego de/para certos endereços IP; o Anomalias de *Logon* – excessivas falhas de *logon, logon* fora do expediente, *logon* a partir de endereços IP não usuais; o Bloqueio de contas e *password scans*; o *Botnets, worms*, DDoD e outros *zero-day malwares*, através do cruzamento dos *logs* de DNS, DHCP e *web proxy*.
• As regras de correlação da solução deverão permitir a detecção de *thresholds* ou utilizar testes e operadores lógicos para correlacionar eventos diferentes, permitindo: o Correlação por detecção de anomalia e padrão de comportamento; o Possibilitar a execução automática de *scripts*, a serem executados em casos "*match*" com a regra de correlação; o Possibilitar a configuração de política de notificação em cada regra; o O ajuste fino de regras de correlação, permitindo identificar as regras mais acionadas por eventos (que geram mais alertas).
• A solução deve ser capaz de correlacionar eventos e fluxos de rede, como NetFlow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução;
• A solução deve realizar a correlação de eventos provenientes das fontes de *logs* e *flows*, resultando na geração de incidentes de segurança.
• A solução deve realizar a correlação dos eventos e *flows*, e a geração de alertas em tempo real;
• A solução deve ser capaz de correlacionar eventos provenientes de múltiplas fontes, tipos ou localizações;
• A solução deve possibilitar a análise de eventos com base em contexto, como usuários, localização geográfica e qualquer outro metadado presente nos eventos;
• A solução deve correlacionar as informações de diferentes fontes de logs e agregar eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes;
• A solução deve oferecer a flexibilidade de utilizar qualquer metadado dos eventos em regras de correlação;
• A solução deve coletar diariamente informações de fontes relevantes de inteligência de ameaças (*Threat Intelligence*) para pesquisar novos tipos de ameaças;

• A solução integrada com o serviço de inteligência de ameaças (*Threat Intelligence*) deverá ter a capacidade de implementar técnicas de reputação categorizadas para no mínimo: o IP's/URL's mal intencionados; o Comportamento de ataque; o Comportamento de *malware*; o Comportamento de *spam*; o URL's de *phishing*; o Atividade de *botnet*; o Atividade de C&C – *Command & Control.*
• A solução integrada com o serviço de inteligência de ameaças (*Threat Intelligence*) deverá processar, normalizar, correlacionar, analisar e armazenar eventos de segurança, de forma escalável, possibilitando análise de ambientes com mais de 30.000 contas de usuários;
• A solução deve ter sua base de inteligência diariamente atualizada através de alimentadores (*feeds*) de informação externos, provenientes da base de conhecimento do fabricante da solução de SIEM, da base de conhecimento da própria CONTRATADA e de pelo menos outras duas fontes de inteligência de terceiros, através do serviço de *feeds* de inteligência e alertas de ameaças direcionadas;
• A solução deve ser capaz de detectar, em tempo real, ameaças alimentadas pelas seguintes bases de inteligência: o proxies anônimos; o endereços de rede TOR; o *botnets* e centros de Comando e Controle; o *malware hosts*; o IP's usados para *scan* de redes.
• A solução deve possuir ferramentas e recursos de caça e investigação proativa de ameaças para identificar e mitigar possíveis riscos de segurança antes que eles aumentem;
• A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que ocorrem ao longo do tempo e não foram previstos ou observados anteriormente;
• A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surtos ou ausência de eventos/tráfego, quando comparados a períodos semelhantes (por exemplo, mesmo período do dia, mesmo dia da semana);

• A solução deve ser entregue com regras de correlação de análise de comportamento de usuários e entidades pré-formatadas, podendo ser utilizado os serviços de customização suportados pelo fabricante e CONTRATADA durante a implantação, devendo processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM quando aplicável, ou devem considerar o total de 30.000 contas monitoradas (contas de usuários + contas de serviços). A monitoração de desvios de comportamento de usuário identificando, no mínimo: o Acesso negado repetido; o Usuário acessando a VPN a partir de uma localidade atípica; o Usuário acessando a VPN a partir de horários atípicos; o Conta utilizada numa quantidade atípica de atividades; o Acesso a endereços considerados suspeitos por bases de *Threat feed*/IP *Reputation*; o Conta de usuário criada e deletada rapidamente; o Detecção de ataque de negação de serviço pela deleção de contas; o Conta anômala em *Cloud*, criada a partir de uma nova localização.
• A solução deve suportar integração nativa com tecnologia de análise comportamental de entidade e usuário (UEBA), baseado em técnicas de *machine learning* ou inteligência artificial, e análises estatísticas para a monitoração de segurança, devendo extrair os dados de usuário e entidades, ações executadas dos eventos coletados para geração de *score* de risco;
• A solução deve possuir recursos, de forma nativo ou através do uso de ferramentas integradas, de análise comportamental de dispositivo e usuários;
• A solução deve utilizar algoritmos de Inteligência Artificial para categorizar e analisar o comportamento das entidades. Entende-se como algoritmos de inteligência artificial no mínimo: o Implementar algoritmos de Inteligência Artificial, incluindo técnicas de aprendizado supervisionado e não supervisionado.
• A solução deve der 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;
• A solução deve implementar IA para Análise Avançada de Ameaças: o Integrar técnicas de processamento de linguagem natural (PLN) para extrair informações relevantes de logs, relatórios de incidentes e outras fontes de dados. o Correlacionar eventos de diferentes fontes para mapear cenários de ataque, determinar o escopo do comprometimento e identificar a raiz das causas. o 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.

• A solução deve implementar IA para Priorização Inteligente de Alertas: o 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. o Permitir a personalização da pontuação de risco de acordo com as necessidades da CONTRATADA, ajustando a importância de cada fator. o Notificar os analistas de segurança sobre alertas críticos em tempo real, facilitando a resposta imediata a incidentes graves.
• A solução deve implementar IA para Investigação Automatizada: o 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. o Gerar insights sobre as investigações, incluindo detalhes sobre a natureza da ameaça, o escopo do comprometimento e recomendar ações a serem tomadas.
• A solução deve implementar IA para Respostas Personalizadas a Incidentes: o 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 CONTRATADA. o Recomendar medidas de mitigação adequadas para conter o incidente, minimizar o impacto nos negócios e prevenir recorrências.
• A solução deve ser capaz de utilizar *Machine Learning* (ML) para estabelecer a linha de base das análises;
• A solução deve possuir recursos nativos de inteligência artificial (IA) ou *Machine Learning* (ML) para a sugestão de *playbooks*, facilitando e automatizando, além de *scripts* para resposta a incidentes;
• A solução deve utilizar diferentes tipos de algoritmos de inteligência artificial para aprimorar sua funcionalidade e desempenho;
• A solução deve possuir métricas de detecção de comportamentos associados a ataques cibernéticos que possam ser detectados imediatamente por mecanismos de inteligência artificial. Essas métricas devem ser de, no mínimo, 50 comportamentos.
• A solução deve utilizar *machine learning* e inteligência artificial para realizar a classificação e mapeamento de informações recebidas de ferramentas de terceiros em tipos de incidentes e campos de incidentes de forma automatizada;
• A solução deve possibilitar investigações ou análise exploratória de dados utilizando algoritmos de Machine Learning ou inteligência artificial, podendo ser nativo ou através do uso de interfaces programáveis como Jupyter Notebook ou similares;
• A solução deve permitir interação do especialista de *cybersecurity* através de interface de conversação que utilize inteligência artificial generativa. Ex.: ChatGPT, Microsoft Copilot, Meta AI, etc;
• A solução deve executar triagem de incidentes, investigação e remediação através de interface de conversação que utilize inteligência artificial generativa;
• A solução deve executar consultas na documentação da solução através de interface de conversação que utilize inteligência artificial generativa;
• A solução deve permitir a definição e customização de alertas, relatórios e gráficos;

• A solução deve possuir integração com serviço de diretório (Microsoft *Active Directory* e protocolo LDAP);
• A solução deve possuir a funcionalidade para resolução de endereços IP, como localização da cidade, país e organização das conexões;
• A solução deve possuir mecanismos para evitar que os alertas fiquem inativos, como monitoramento contínuo e reativação automática de alertas não resolvidos;
• A solução deve possuir serviço de monitoração de estado de recebimento e/ou processamento de *logs*/eventos;
• A solução deve identificar análise incorreta ou incompleta de dados de log;
• A solução deve permitir que os logs/eventos sejam enriquecidos/categorizados com informação de criticidade/severidade;
• A solução deve atribuir uma métrica de prioridade tanto para os eventos quanto para os alertas/incidentes;
• A solução deve oferecer a capacidade de controlar ou substituir a urgência do alerta com base em fatores como caso de uso, ativo ou identidade envolvidos na atividade;
• A solução deve oferecer a possibilidade de salvar o resultado de pesquisa (*query*) em casos de uso, indicadores de comportamento ou tipos de alertas;
• A solução deve notificar através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
• A solução deve possibilitar a agregação de eventos similares;
• A solução deve possuir um painel de controle (*Dashboard*), onde através de simples "*drill-down*" possa ver o *log*/evento coletado;
• A solução deve fornecer painel de controle (*Dashboard*) que constantemente mostre o status do ambiente de correlação de eventos;
• A solução deve permitir que, a partir de uma informação existente, se verifique o *log* que a gerou através de recurso de "*drill-down*";
• A solução deve permitir a análise avançada de eventos, podendo correlacionar eventos em uma base histórica;
• Suportar análise de atividade de rede usando protocolos como NetFlow ou IPFIX;
• A autodetecção da solução deverá ser capaz de possibilitar a busca de eventos, com os seguintes recursos mínimos: o Busca em tempo real, baseada em "Google-*like keywords*" ou "SQL-*like structured queries*"; o Possibilidade de converter os resultados procurados em relatórios ou dashboard widgets; o Suportar o relacionamento de ativos tecnológicos com os processos de negócio, com a respectiva relevância do primeiro em relação ao segundo.
• A solução deve possuir procedimento de *Backup & Restore* para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador na nuvem do FABRICANTE;

• A solução deve suportar de forma nativa e automática o armazenamento online (dados presentes no *storage* da solução por 3 meses) e offline (dados presentes em sistemas de armazenamento *off-line, backup*, por 9 meses para possível restauração online);
• A solução deve possuir procedimento de *Backup & Restore* para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador local físico na infraestrutura da CONTRATANTE, para armazenamento dos dados gerados durante o período do edital;
• A solução deve suportar algoritmos de compressão nos sistemas de armazenamento de longo prazo;
• A solução deverá enviar ou fornecer acesso a um ambiente em nuvem que possibilite baixar os logs brutos para o arquivador físico da CONTRATANTE, devendo: o O ambiente deverá armazenar de forma indexada esses logs em formato texto (JSON, XML, CSV ou TXT) compactado (xz, gzip, bzip2 ou lzop) por no mínimo 7 (sete) dias; o A transferência dos logs deverá ser realizada por meio de canais seguros, utilizando protocolos de criptografia adequados para garantir a integridade e a confidencialidade dos dados durante o processo; o Os arquivos poderão, a critério da contratante, ser importados e indexados pela solução ofertada permitindo análise dos dados no ambiente da ferramenta; o Todo o serviço de envio dos logs para o arquivador físico da CONTRATANTE deverá ser realizado pela CONTRATADA, com acompanhamento da equipe técnica da CONTRATANTE.
• A solução deve permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;
• Todos os dados coletados ou gerados durante a prestação dos serviços são de propriedade da contratada, devendo: o Ao final do contrato, todos os dados gerados deverão ser transferidos para o ambiente da CONTRATANTE; o Após confirmação de recebimento e integridade dos dados, a contratada deverá proceder com a exclusão completa dos dados de seus sistemas, mediante solicitação formal do contratante; o O procedimento de destruição dos dados poderá ser acompanhado pela equipe técnica da CONTRATANTE.
• A solução deve permitir a exportação de logs/eventos armazenados no mínimo em 2 (dois) dos seguintes formatos: texto, XML, JSON, TSV ou CSV;
• A solução deverá permitir auditorias periódicas para verificar a conformidade com os requisitos de transferência e exclusão de dados;
• A solução deve possuir integração com soluções de gerenciamento de postura de segurança em nuvem (CSPM) para monitoramento contínuo de segurança e aplicação de conformidade em ambientes de nuvem;
RELATÓRIOS
• A solução deverá permitir a geração de relatórios manuais e automatizados, possuindo funcionalidade de agendamento e envio por *e-mail*;
• A solução deve permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
• A solução deve segregar a visualização de relatórios apenas para usuários com a devida permissão;

• A solução deve permitir a construção de relatórios customizados pelo usuário;
• A solução deve permitir que o administrador possa filtrar *logs*/eventos ao gerar relatórios;
• A solução deve possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
• A solução deve permitir a customização de novos relatórios baseados em dados de *Logs* e *Flows* de rede;
• A solução deve possibilitar a personalização de novos relatórios com base em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes;
• A solução deve criar *dashboards* e relatórios para acompanhar a conformidade com auditorias e controles internos;
• A solução deve permitir visualização facilitada dos dados de auditoria da própria solução, podendo ser através de relatórios, *dashboard* ou painéis;
• A solução deve criar *dashboards* e relatórios para acompanhar a conformidade com práticas internacionais e desempenho da operação de *cybersecurity;*
• A solução deve criar *dashboards* e relatórios focados em regulamentações e padrões do setor, como GDPR ou PCI DSS;
• A solução deve possuir relatórios de conformidade com a ISO-27001;
• A solução deve permitir integração com ferramentas de gerenciamento de conformidade para avaliações e relatórios automatizados de conformidade da solução;
• A solução deve exibir *dashboard* em tempo real sobre a ingestão dos logs e informações, categorizando no mínimo em produtos e fabricante;
• A solução deve criar *dashboards* e relatórios com métricas padrões para tempo médio de detecção (MTTD) e tempo médio de resposta (MTTR);
• A solução deve possuir relatórios voltados para análise de eventos de Firewall, antivírus e IPS;
• A solução deve permitir a geração de relatórios que incluam os eventos associados a um incidente detectado por regras de correlação;
• A solução deve contar com a opção de incluir os TOP endereços lógicos de origem das ameaças, TOP países e cidades de origem das ameaças e dos alertas de segurança;
• A solução deve possuir relatórios que suportem a gestão das fontes de eventos, como *data sources* com erro;
• A solução deve permitir gerar relatórios em pelo menos um destes formatos: HTML, PDF ou CSV;

- A solução deverá possuir alguns relatórios pré-formatados, e possibilitar a exportação em pelo menos um dos formatos CSV, PDF, MHTML, Excel ou Word, para no mínimo:
  - Incidentes abertos por fase;
  - Incidentes Encerrados por Duração;
  - Incidentes Abertos Por Duração;
  - Incidentes Abertos por severidade;
  - Incidentes reabertos;
  - Falso positivo por Solução;
  - Tempo Médio de resolução por tipo de incidente;
  - Tempo Médio entre o Alerta e o primeiro tratamento por tipo de incidente;
  - Incidentes com SLA expirado por tipo de Incidente;
  - Incidentes com SLA expirado por responsável.

2.2 SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SIEM – (ITEM 2)

- Serviços de apoio à customização e implementação da solução - planejamento da implantação, instalação e configuração da solução;
- Todas as atividades relacionadas à instalação e configuração das soluções ofertadas serão prestadas nas instalações do Centro Administrativo Presidente Getúlio Vargas (CAPGV) do Banco do Nordeste do Brasil, situado em Fortaleza-CE, à exceção das atividades que envolvam diagnóstico e solução de problemas durante a implantação, as quais poderão ser realizadas por equipe remota, desde que acompanhadas nas instalações do CAPGV por equipe técnica da CONTRATADA;
- Todas as atividades relacionadas à implantação ocorrerão sob a responsabilidade e expensas da CONTRATADA, sem nenhum ônus adicional para o Banco, cabendo a este somente o apoio técnico e a avaliação dos resultados, nos termos previstos neste Edital;
- Por instalação, configuração, integração e ativação entendam-se todos os procedimentos relacionados à implantação e configuração (lógica), parametrização e testes de quaisquer componentes da solução ofertada, além de realizar a integração entre as ferramentas de segurança do Banco do Nordeste, de modo a garantir o pleno funcionamento dos mesmos;
- Todos os componentes requeridos para atender às funcionalidades exigidas neste Edital devem estar especificados na proposta;
- A CONTRATADA deverá configurar o ambiente em nuvem que possibilite baixar os logs brutos para o arquivador físico da CONTRATANTE, com acompanhamento da equipe técnica da CONTRATADA;
- A CONTRATADA deve criar e manter atualizada a documentação das atividades, dos processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, atas de reuniões, de modo a compor uma documentação final da implantação a ser entregue ao Banco no final do processo;

- A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de apoio a customização e implementação da solução, objeto deste Edital. Caso o diagnóstico aponte para problemas não relacionados aos serviços de apoio a customização e implementação da solução, o Banco deverá executar os referidos procedimentos, desde que devidamente comprovados pelo Contratado, e a critério do Banco.
- A CONTRATADA deve, às suas expensas, alocar toda a equipe que irá instalar, configurar, integrar e executar os serviços de implantação descritos neste Edital;
- Deverão ser alocados, pela CONTRATADA, no mínimo, 3 (três) profissionais qualificados para acompanhar o planejamento e a execução dos serviços de implantação e integração dos componentes da solução, distribuídos da seguinte forma: no mínimo 2 (dois) profissionais com perfil técnico e no mínimo 1 (um) profissional com perfil de gestão de projetos;
- A equipe alocada pela CONTRATADA deverá realizar as atividades do projeto, de forma presencial, nas dependências do CAPGV, no mínimo, nas quantidades de horas descritas abaixo:
    - Profissionais com PERFIL TÉCNICO: 8 (oito) horas diárias, cada um, em horário comercial, durante todo o período de PLANEJAMENTO e EXECUÇÃO da implantação e integração da solução, desde a construção da versão inicial do Plano de Implantação e Integração até a emissão do TAD (Termo de Aceitação Definitiva);
    - Profissional com PERFIL GESTÃO DE PROJETOS: 8 (oito) horas diárias, em horário comercial, durante todo o período de PLANEJAMENTO da implantação e integração da solução, desde a construção da versão inicial do Plano de Implantação e Integração, até a emissão do TAP (Termo de Aceitação Provisório);
- Dentre os profissionais alocados de forma presencial, a CONTRATADA deverá indicar um Gerente de Projetos, com certificação PMP – Project Management Professional do PMI – *Project Management Institute* ou possuir MBA – *Master of Business Administration* em Gerência de Projetos, que será o líder e responsável pela entrega dos serviços e pela gestão da implantação e integração da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital;
- Todas as despesas referentes a transporte, alimentação, hospedagem e demais despesas operacionais da equipe alocada pelo Contratado ocorrerão às suas expensas;
- O Banco disponibilizará estrutura adequada no local de trabalho, incluindo estações, acesso físico às suas instalações e identificação através de crachás, bem como autorização, acesso aos recursos computacionais e de apoio técnico às atividades de implantação, desde que absolutamente dentro do escopo das atividades da equipe do Banco e a seu critério.
- O Banco se reserva o direito de redefinir, a qualquer momento da implantação, quaisquer fases, ações e prazos envolvidos, objetivando a garantia de atendimento dos parâmetros de qualidade, segurança, mitigação de riscos e atendimento de prazos, cabendo ao Contratado adequar-se às modificações propostas, refazendo atividades e documentação, caso seja necessário, desde que essas não extrapolem o escopo dos serviços aqui descritos;

• O Contratado deve apresentar ao Banco, em reunião própria, documento que balizará o acompanhamento de todo o projeto de implantação, em formato Microsoft Project, detalhando todas as fases, atividades, ações, recursos envolvidos (humanos e materiais), prazos, interdependências entre fases, atividades e ações, linha crítica temporal da implantação e quais serão os produtos gerados para cada fase, atividade e ação;
• O Contratado deve submeter o Plano de Implantação à homologação por parte do Banco, reservando-se este o direito de requerer os ajustes necessários, observadas as melhores práticas amplamente aceitas no mercado e a realidade de seu ambiente;
• O Contratado deve implementar, no Plano de Implantação, todos os ajustes que venham a ser solicitados pelo Banco e apresentar a nova versão;
• Os serviços de implantação contemplarão, pelo menos, a realização das seguintes macrofases: o Implantação da solução e configuração de cada componente ofertado; o Integração da ferramenta de SIEM ao ambiente do BANCO DO NORDESTE, conforme descrito no **Anexo VI – Plataforma Computacional**; o Configuração de, no mínimo, 30 regras de correlação, previamente aprovadas pelo BANCO DO NORDESTE; o Configuração e operacionalização do modulo de gestão de incidentes para registrar e escalar eventos de segurança; o Configuração da transferência periódica dos logs coletados, de forma comprimida, para o arquivador físico da contratante; o Período de funcionamento experimental;
• O Gerente de Projetos da CONTRATADA deve comunicar ao gestor do Banco responsável pelo acompanhamento da implantação dos serviços a conclusão de cada macro-fase;
• O plano de implantação deve considerar os prazos e interdependências entre fases previstos no Anexo III – Plano de Implantação;
2.3 SERVIÇO ESPECIALIZADO DE ADMINISTRAÇÃO E SUPORTE À FERRAMENTA OFERTADA – (ITEM 3)
• A CONTRATADA deverá prover serviços de administração e suporte à solução de coleta e correlação de logs e eventos de segurança da informação (SIEM), integrada a serviços de inteligência de ameaças (*Threat Intelligence Feeds*) e seus demais módulos, conforme especificado no item 1;
• Deverá ser alocado, pela CONTRATADA, no mínimo, 2 (dois) profissionais certificados na solução de SIEM ofertada, para realizar as atividades conforme os seguintes perfis: o Perfil I: Administração e suporte à solução, de forma presencial, por, no mínimo, 8 (oito) horas diárias, em horário comercial; o Perfil II: *Thread hunting*, de forma presencial, por, no mínimo, 8 (oito) horas diárias, em horário comercial;
• A CONTRATADA deve utilizar analistas capacitados e certificados na solução de SIEM fornecida para realizar as atividades descritas;

- A CONTRATADA deverá realizar todas as operações de administração, gerenciamento, *hunting* e monitoramento das ferramentas ofertadas, incluindo, mas não se limitando a:
    - Perfil I - Administração e suporte à solução:
        - Coleta de logs;
        - Realização de configurações;
        - Interação com o fabricante da solução ofertada;
        - Interação com a equipe técnica do Banco do Nordeste responsável pela configuração do envio de logs nos ativos monitorados;
        - *Backup* e *restore*;
        - Criação de relatórios e dashboards;
        - Resolução de problemas;
        - Atualização, de acordo com as recomendações do fabricante;
        - Performance e bem-estar da solução;

    - Perfil II - *Thread hunting*:
        - Criação de regras de correlação, não havendo limites mínimo ou máximo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados;
        - Definição de vetores de ameaça;
        - Melhoria contínua das regras de correlação;
        - Interação com o fabricante da solução ofertada;
        - Interação com a equipe técnica do Banco do Nordeste responsável pela análise e resposta de incidentes;
- A CONTRATADA deverá apresentar um conjunto de regras pré-estabelecidas para ativação. Estas regras somente serão implementadas após a aprovação do Banco do Nordeste;
- O Banco do Nordeste irá realizar a configuração em seus equipamentos para enviar os logs para a solução de SIEM, sendo responsabilidade da CONTRATADA realizar as configurações na solução de SIEM;
- A CONTRATADA é responsável pela execução de todas as atividades de gestão, manutenção, configuração, suporte e administração na Solução Integrada de SOC;
- A CONTRATADA deve manter atualizados os módulos da Solução Integrada de SOC, instalar *patches*, correções e versões ou releases mais recentes dos *softwares*, provisionamento dos serviços de configuração e implementação de facilidades de configuração para atualização ou modificação dos recursos lógicos dos módulos da solução;
- A CONTRATADA deve executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos módulos da Solução Integrada de SOC fornecida;

- A CONTRATADA deve monitorar, analisar e controlar o desempenho de cada componente da Solução Integrada de SOC fornecida, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução, substituindo-os sem custo adicional ao Banco do Nordeste, caso necessário;
- A CONTRATADA deve executar procedimentos para fazer o ajuste fino (*tunning*) de toda a Solução Integrada de SOC, adequando-a ao ambiente do Banco do Nordeste e realizando as customizações de configuração necessárias;
- A CONTRATADA deve realizar a gerência de segurança da Solução Integrada de SOC, sendo responsável pela proteção das informações, restringindo o acesso à rede e impedindo o uso incorreto por parte de seus usuários, de forma intencional ou não;
- A CONTRATADA deve realizar as operações de administração na Solução Integrada de SOC para solicitação de criação de contas de acesso para os analistas do Banco do Nordeste, solicitação de registros de auditoria da ferramenta ou outras configurações solicitadas pelo Banco do Nordeste. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;
- A CONTRATADA deve configurar os perfis de acesso diferenciados, necessários para que os analistas do Banco do Nordeste utilizem todos os serviços contratados.
- A CONTRATADA deve fornecer possibilidade de perfis que permitam acesso a qualquer informação armazenada na Solução Integrada de SOC;
- A CONTRATADA deve fornecer, sob demanda do Banco do Nordeste, relatório contendo a lista de usuários cadastrados na ferramenta, o perfil de acesso, situação da conta e última data de acesso;
- A CONTRATADA deve realizar a integração assistida dos sensores de segurança do Banco do Nordeste com a Solução Integrada de SOC fornecida, sempre que solicitada. Essa atividade corresponde minimamente a:
    - Definir o método de coleta de dados, analisando as interfaces e protocolos suportados pelos sensores de segurança (syslog ou protocolos específicos do fabricante);
    - Definir os procedimentos que devem ser executados nos sensores de segurança, definindo os atributos da fonte de dados e parâmetros que devem ser habilitados para operacionalizar o envio dos dados à Solução Integrada de SOC;
    - Normalizar, agregar e executar o *parsing* dos dados, logs e alertas capturados, realizando todas as configurações necessárias para mapear os dados para um formato comum que possa ser utilizado nas regras de correlacionamento da Solução Integrada de SOC;
    - Realizar todas as configurações necessárias na Solução Integrada de SOC para habilitar a aquisição dos dados dos sensores;

• A CONTRATADA deve realizar a transferência periódica dos logs coletados para o ambiente *on-premise* do contratante, em formato legível e estruturado. Essa atividade corresponde minimamente a: o A configuração, o monitoramento e manutenção desse processo contínuo serão de responsabilidade da CONTRATADA, com o devido suporte técnico da CONTRATANTE. o Auditorias periódicas para verificar a conformidade com os requisitos de transferência e exclusão de dados, bem como fornece relatórios detalhados sobre as operações realizadas. o A contratada será responsável por garantir que todos os dados transferidos estejam completos e íntegros, incluindo todos os dados gerados até a data final de vigência contratual, assumindo a responsabilidade por qualquer perda ou corrupção de dados durante o processo de transferência.
• A CONTRATADA deve definir em comum acordo com o Banco do Nordeste o método mais eficiente para a coleta de dados dos sensores de segurança, de forma a não prejudicar a performance dos sensores de segurança. O procedimento proposto só será aceito após avaliado pelo Banco do Nordeste;
• A CONTRATADA deve realizar esta atividade durante toda a vigência do contrato, cabendo ao Banco do Nordeste solicitar a inclusão ou retirada de sensores integrados, inclusive para novos sensores adquiridos pelo Banco do Nordeste após a definição da lista inicial. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;
• O sensor é considerado integrado à solução quando seus dados estiverem disponíveis para correlacionamento e monitoração em tempo real pela ferramenta da Solução Integrada de SOC. A CONTRATADA deve fornecer um relatório contendo evidências da integração de cada sensor de segurança;
• As regras de correlacionamento utilizam informações adquiridas de múltiplos sensores de segurança gerando alertas mais qualitativos, de forma a melhorar o monitoramento de segurança, simplificando a identificação de incidentes ou falhas de segurança. A correlação de eventos é a forma mais conhecida e utilizada de análise de dados, criando contexto e revelando relacionamento entre eventos recebidos de diversas fontes, com o objetivo de identificar e reportar ameaças. O contexto pode ser por tempo, endereço de origem ou destino, valor dos ativos, por heurísticas ou outros critérios;
• A CONTRATADA deve realizar a configuração das regras na Solução Integrada de SOC fornecida, de forma proativa ou sempre que solicitada pelo Banco do Nordeste, permitindo a detecção de ameaças direcionadas ao ambiente do Banco do Nordeste;

• A CONTRATADA deve configurar proativamente regras de correlacionamento, baseadas em boas práticas de segurança e bases de conhecimento próprias, customizadas para o ambiente do Banco do Nordeste, monitorando minimamente: o Detecção de anomalias de comportamento com base em alterações em uma linha de base; o Detecção de anomalias de comportamento baseado em estatísticas (*Statistical Behavioral Analysis*); o Detecção de anomalias com base em tendências (*Trend Behavior Analisys*); o Detecção de padrões em logs observados e não observados; o Detecção de padrões baseados em uma sinalização específica (*thresholds*); o Detecção de padrões baseados em valores unitários; o Detecção de ameaças que saem de normas básicas (*whitelisting*);
• A CONTRATADA deve manter as regras atualizadas, de modo a refletir a ocorrência de novas ameaças, novas políticas de alarme, atualizações de padrões de logs de tecnologias ou escopo monitorado;
• A CONTRATADA deve fornecer base de conhecimento de métricas, indicadores de intrusão ou de comprometimento, atualizadas periodicamente de acordo com a mudança do cenário de ameaças e surgimento de novas técnicas ou padrão de ataque, permitindo monitorar e analisar mudanças no comportamento do usuário, rede ou aplicações, que podem significar uma atividade maliciosa;
• O Banco do Nordeste pode solicitar, a qualquer momento, a implementação de regras de correlacionamento a serem implementadas na Solução Integrada de SOC, baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar as regras na solução. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;
• O Banco do Nordeste não deve realizar a edição de regras de correlacionamento sem o conhecimento da CONTRATADA;
• O Banco do Nordeste deve fornecer dados de inteligência de negócio (características dos sensores, ativos e aplicações), como subsídios para que a CONTRATADA possa otimizar todas as regras de correlacionamento implementadas, de forma a reduzir o número de falsos positivos e melhorar a eficiência dos alarmes. Os dados fornecidos serão os mínimos necessários para a atividade, respeitando todas as restrições impostas pela legislação vigente e normativos internos do Banco do Nordeste;
• A CONTRATADA deve realizar a configuração dos painéis e relatórios de monitoramento na Solução Integrada de SOC fornecida, de forma proativa ou sempre que solicitada pelo Banco do Nordeste;
• A CONTRATADA deve configurar um conjunto básico de painéis, contendo indicadores definidos de acordo com suas bases de conhecimento próprias, customizadas para o ambiente do Banco do Nordeste;
• O Banco do Nordeste pode solicitar, a qualquer momento, a implementação de painéis ou relatórios para apresentar indicadores próprios definidos baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar os painéis na solução. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

• O Banco do Nordeste pode solicitar acesso a qualquer dos painéis ou relatórios configurados na ferramenta, de acordo com o nível de acesso que o Banco do Nordeste definirá para cada um de seus analistas autorizados a acessar a Solução Integrada de SOC;
• O Banco do Nordeste pode solicitar perfil de acesso aos seus analistas que possibilitem a construção de painéis e relatórios customizados, visualização e a filtragem dos eventos e alertas na Solução Integrada de SOC;
2.4 SERVIÇO DE MONITORAÇÃO E NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA – (ITEM 4)
• O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), com raio de distanciamento de 300km entre eles;
• A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica: o Solução de proteção de endpoints; o Solução de prevenção contra vazamento de informações (DLP); o Solução de proteção de e-mails; o Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria; o Efetue o registro dos visitantes com identificação individual e controle digital de entrada e saída, mantendo o registro armazenado e disponível para consulta por 90 dias; o Monitoramento por equipe de segurança patrimonial em regime 24x7x365; o Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 90 (noventa) dias; o Possua uma das certificações ISO 27001 ou ISO 27701 no seu Centro de Operações de Segurança (SOC); o Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do Banco devem assinar termo de responsabilidade e sigilo;
• A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança realizado por seus analistas, em regime 24 X 7 (24 horas por dia, 7 dias da semana);
• A CONTRATADA deve realizar as ações necessárias para identificação de incidentes de segurança por meio dos dados e alertas monitorados na Solução Integrada de SOC, que podem comprometer a segurança dos serviços e ativos do Banco do Nordeste. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição do Banco do Nordeste, bem como identificar, registrar, escalar e notificar os incidentes de segurança ao Banco do Nordeste para tratamento;
• A CONTRATADA é responsável pelas atividades de camada 1 do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

○ **Definição de linha base** (*baseline*) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção.
○ **Monitoração de alertas de segurança**, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no *baseline*. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente: ▪ Ataques de força bruta com e sem sucesso; ▪ Falhas de autenticação que indiquem suspeita de roubo de identidade; ▪ Infecção de equipamentos por vírus; ▪ Comprometimento de ativos da rede; ▪ Realização de ações suspeitas por parte de usuários privilegiados; ▪ Alertas de operação de serviços, como interrupções e falhas; ▪ Ataques de negação de serviço; ▪ Ataques comuns em aplicações WEB, como XSS e *SQL injection*; ▪ Atividades de *botnets*; ▪ Exploração de vulnerabilidades;
○ **Detecção por análise de logs**, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.
○ **Análise de eventos**, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias: ▪ Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes; ▪ Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são; ▪ Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades; ▪ Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

○ **Registro de análise**, todo evento detectado que for selecionado para análise deve ser registrado no Sistema de Ticket ofertado, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações: ▪ Identificador do ticket; ▪ Sensor que detectou o evento; ▪ Identificador do evento gerado no sensor; ▪ Limiar de detecção utilizado para enviar o evento para análise; ▪ Log do evento detectado; ▪ Origem e categoria do ataque; ▪ Data e hora;
○ **Triagem e Categorização de eventos**, os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas do Banco do Nordeste;
○ **Padronização de procedimentos de resposta à incidentes**, os incidentes escalados devem incluir procedimentos padronizados contendo as melhores práticas para seu tratamento e contenção, de modo que viabilize a execução das medidas corretivas necessárias pelo Banco do Nordeste. Esses procedimentos são orientados para incidentes aplicáveis a ambientes genéricos ou que constem da base de conhecimento da CONTRATADA;

○ **Elaboração de relatórios**. A CONTRATADA deverá disponibilizar relatórios em formato pdf, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir: ▪ Classificação dos eventos de segurança; ▪ Total de eventos avaliados; ▪ Total de eventos escalados; ▪ TOP aplicações mais impactadas, TOP origens dos eventos de segurança; ▪ TOP endereços de destino das ameaças; ▪ TOP URLs e suas categorias; ▪ TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria; ▪ Principais tipos de ataques; ▪ Descrição dos casos de uso utilizados para avaliar os alertas de segurança; ▪ Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, *dashboards*, assinaturas instaladas, etc;
• O Sistema de Ticket ofertado deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes do Banco do Nordeste e da própria CONTRATADA;
• O Banco do Nordeste é responsável por avaliar os incidentes escalados após o processo de triagem inicial. Caso o incidente seja confirmado, o Banco do Nordeste executará os seus processos e procedimentos internos para executar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos. O Banco do Nordeste registrará as ações realizadas no tíquete correspondente ao incidente, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo;
• Os analistas do Banco do Nordeste responsáveis pelos tíquetes escalados devem possuir acesso total as informações do incidente relacionado;
• Os analistas do Banco do Nordeste devem poder contatar os analistas da CONTRATADA, por telefone ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
• O Banco do Nordeste é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;
• O Banco do Nordeste pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar a customização. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

• Por padrão, a CONTRATADA não deve possuir nenhum tipo de acesso aos ativos, sensores e ferramentas de proteção do Banco do Nordeste. Em casos específicos e por tempo determinado, caso autorizado pela área de segurança do Banco do Nordeste, pode ser fornecido acesso de leitura de registros do IPS, dados de sessão de rede (flow) e outras ferramentas de segurança para auxiliar em pesquisas pontuais de eventos de segurança. Não será fornecido nenhum tipo de acesso a dados ou sistemas do Banco do Nordeste, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;
• A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia do Banco do Nordeste. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente do Banco do Nordeste;
• A CONTRATADA deve fornecer e, quando solicitado pelo Banco, apresentar: o Boletins periódicos, baseados nas informações de dados globais dos centros de pesquisa de ameaças, contendo novas táticas e técnicas de ataque, vulnerabilidades e mecanismos de proteção de interesse do Banco do Nordeste; o Relatórios mensais especializados para o ambiente do Banco do Nordeste, incluindo informações de inteligência, como as novas vulnerabilidades identificadas, ameaças direcionadas identificadas, indicadores de ataque, reputação de endereços IP e domínios, indicadores sobre o cenário de segurança monitorado do Banco do Nordeste; o Relatório anual sobre a implementação do plano de ação e de resposta à incidentes, conforme é definido na Resolução CMN n.º 4.658 e demais regulamentações; o Identificação, análise e compartilhamento de informações de ameaças relevantes e emergentes por meio de indicadores de comprometimento;
2.5 SERVIÇO ESPECIALIZADO DE APOIO À GESTÃO DO SOC – (ITEM 5)
• Este serviço tem como objetivo apoiar a gestão do SOC, visando a definição, implementação e aprimoramento de processos e metodologias aplicáveis à administração do SOC;
• Deverá ser realizado com abordagem agnóstica, ou seja, independente das tecnologias de segurança e fabricantes;
• Deverá ser realizado por profissional(is) com perfil especialista, com experiência comprovada em administração de SOC;
• Fazem parte do escopo do serviço especializado de apoio à gestão do SOC as seguintes atividades:
o Revisar as definições de negócio e objetivos do SOC;
o Elaborar, documentar políticas de segurança, normas, procedimentos, guias e processos conforme as definições de negócio e objetivos do SOC;

○ Apresentar recomendações para atualização das normas internas e da política de segurança do Banco, necessárias para refletir as definições instituídas para o funcionamento do SOC;
○ Apoiar no desenvolvimento de estratégias de segurança cibernética para suportar a transformação digital, apresentando recomendações contextualizadas e referenciadas;
○ Definir e documentar diretrizes de gerenciamento de risco de segurança cibernética de acordo com a legislação vigente, por exemplo, com base nas resoluções do Bacen n.º 4.893 e 4.557, normas ISO e programas de compliance;
○ Definir e documentar estratégia para o gerenciamento de desempenho do SOC, medição do grau de maturidade, criando abordagem estratégica para acompanhar sua evolução, ou seja, avaliar o estado atual, estabelecer o estado destino e identificar as ações necessárias para atingir o estado destino do SOC, englobando todos os pontos da estrutura (pessoas, processos e tecnologia) identificando oportunidades de melhorias e definindo o plano de ação para elevar a maturidade do SOC;
○ Realizar avaliação de maturidade do SOC anualmente para a identificação das lacunas (gaps) no âmbito de processos, pessoas e tecnologia e propor recomendações de estratégia e plano de ação para o tratamento;
○ Avaliar os controles de segurança existentes (resiliência frente as ameaças), disponibilidade das informações para identificação de ameaças, processos de comunicação e, não obstante, silos de segurança da informação existentes nas áreas de negócio e TI;
○ Definir e documentar metodologia de criação e de gerenciamento de métricas e indicadores de desempenho;
○ Definir e documentar processo de monitoramento de performance do SOC;
○ Definir e documentar métricas de desempenho, indicadores chave (KPIs), métricas e análises de eficiência para impulsionar o trabalho, exemplificar a aplicação do uso destas para vincular o risco de segurança ao risco de negócio de maneira a apoiar a discussão dos custos e benefícios de segurança com os executivos, gestão de capacidade do SOC, esclarecer sobre a postura de segurança do Banco (ameaça e resposta);
○ Definir diretrizes para documentação e geração de relatório, modelos e procedimentos, e também modelos para cada caso macro identificado;
○ Definir e documentar modelo simplificado para documentação de procedimentos e diagramas de fluxos;
○ Definir diretrizes de design e manutenção do SOC;
○ Definir e documentar estratégias para escalabilidade horizontal e vertical dos recursos, componentes do ambiente, arquitetura e equipe;
○ Elaborar manual de operações do SOC, descrevendo: diretrizes, processos e procedimentos sobre o funcionamento e controles da estrutura;
○ Definir e documentar política de gerenciamento de eventos, contendo as diretrizes relacionadas a geração, coleta, retenção, classificação e monitoramento de logs;
○ Definir e documentar diretrizes para a gestão de incidentes de segurança;

○ Apresentar recomendações sobre a gestão compartilhada das ferramentas de segurança, apresentando recomendações contextualizadas e referenciadas, considerando, no mínimo, aspectos de integrações, autonomia dos níveis de atuação envolvidos, customizações e automatizações;
○ Gerar recomendações aplicáveis para ampliar a cobertura e visibilidade do ambiente e para implementar procedimentos de resposta automatizada em *endpoints*;
○ Definir e documentar norma e procedimentos para definição de casos de uso e elaboração dos planos de resposta a incidentes (*playbooks*);
○ Apoiar na definição dos papéis, responsabilidades e dimensionamento adequado da equipe de operação do SOC;
○ Suporte consultivo em momentos de crises cibernéticas para executivos e técnicos;
○ Orientar sobre o uso de fontes de inteligência de ameaças contextualizadas (*Threat Intelligence*), e uso da abordagem de caça (*Threat Hunting*);
○ Definir e documentar estratégias para o uso dos entregáveis do serviço de visibilidade de ameaças pelo SOC, de maneira a garantir o atendimento, a análise de inteligência de segurança (exemplo, comparar os padrões globais de ataque com o ambiente interno, analisar as informações do vetor de ameaças aplicáveis) e atendimento à inteligência do negócio (exemplo, mapeamentos críticos, análises de impacto, principais riscos, alinhamento com as políticas corporativas, conformidade normativa e/ou mercado e obrigações legais);
○ Definir rotinas de visibilidade de ameaças para identificação de novos casos de uso, abrangendo, por exemplo: SIEM, Scan de vulnerabilidades, proteção de perímetro, projetos de segurança, apontamentos de auditorias, dentre outros;
○ Definir e documentar estratégia de desenvolvimento e retenção de talentos em *cybersecurity* para o SOC;
○ Entender sobre requisitos regulatórios, contratuais, legais e padrões da indústria financeira que se referem à segurança da informação, exemplo: crimes cibernéticos e violação de dados, licenciamentos, privacidade, utilização de nuvem, dentre outros;
○ Orientar sobre a aplicabilidade e utilização de *frameworks* de segurança, exemplo: indicados pelo NIST, Mitre, *Cyber Kill Chain*, ATT&CK, dentre outros;
○ Entender e aplicar conceitos de gerenciamento de riscos, tipos aplicáveis de controles para prevenção, detecção e correção, seleção e implementação de contramedidas, monitoramento e medição, avaliação de controles de segurança, *frameworks* de riscos, valoração de ativos, dentre outros;
○ Identificar os caminhos críticos na segurança das informações, identificando pontos de vulnerabilidades, para embasar planos de ação e elaboração dos *playbooks*;
○ Desenvolver e documentar escopo e planejamento para análise de riscos sob o prisma de tecnologia, proteções em camadas;
○ Desenvolver e documentar estratégias para apoiar as atividades de gerenciamento de patches e tratamento de vulnerabilidades;
○ Entender e aplicar conceitos e metodologias de modelagem de ameaças;
○ Recomendar ações, revisar e acompanhar o progresso de planos de ação preventivos e corretivos sob contexto de atuação do SOC;

○ Avaliar a estrutura do SIEM, no que tange à abrangência das regras, alertas, dashboards, *data sources*, automatizações, relatórios, dimensionamento para atender aos objetivos do SOC e alinhamento com os casos de uso;
○ Apresentar recomendações para gestão do SIEM, indicando melhores práticas com foco em atendimento aos objetivos do SOC, norteando ações necessárias para que o SIEM forneça um ambiente com recursos adequados, promovendo uma plataforma eficiente com precisão para suportar as funções de monitoramento e análises do SOC, participar da elaboração do plano de ação e da implementação;
○ Avaliar o resultado do *health check* periódico da solução de SIEM e apresentar apontamentos e recomendações;
○ Desenvolver e documentar estratégias para o gerenciamento de segurança da informação e eventos (SIEM), contemplando atividades de registro, lógica para correlações, monitoramento e alertas;
○ Entender e aplicar conceitos de avaliação e testes de segurança para projetar e validar estratégias de condução e análise de resultados dos exercícios dos *playbooks*;
○ Desenvolver exercícios dos *playbooks* envolvendo as diversas equipes para facilitar a prática de resposta apropriada e oportuna, realizar atividades estratégicas para manter a consciência das tendências relacionadas ao ambiente do plano e ao cenário geral de ameaças, permitindo, assim, testar o plano de resposta à incidentes de segurança, bem como o entendimento deste plano pela equipe de segurança envolvida;
○ Participar dos exercícios dos *playbooks*, apresentar apontamentos e recomendações de melhoria;
○ Entender e apoiar investigações de operações de segurança, coleta, manuseio de evidências, técnicas de investigação, tipos de investigação, táticas e procedimentos de forense digital, relatórios e documentação;
○ Apoiar na condução de gerenciamento de incidentes, atividades de prevenção, detecção, resposta, mitigação, remediação e lições aprendidas, provendo assessoria na gestão e na resolução de incidentes de segurança;
○ Assessorar a coordenação de resposta a incidentes, provendo apoio à equipe técnica do Banco, podendo: a) Orientar sobre a execução de procedimentos; b) Proceder com acionamento de recursos, por exemplo: sala de crise e sala de controle;
○ Participar em processos de gerenciamento de mudanças, sob o contexto de atuação do SOC;
○ Definir casos de uso e procedimentos reativos para atender aos objetivos do SOC, elaborando os respectivos *playbooks*;
○ Participar das tratativas, reuniões, negociações com as áreas (TI e Negócio) envolvidas, para levantamento das informações necessárias à definição e implementação das estratégias de detecção e resposta à incidentes de segurança;
• A CONTRATANTE deve apoiar a criação de casos de uso que descrevem cenários de maneira a modelar o comportamento em nível de estratégia, auxiliam na captura de requisitos e descrevem alternativas de decisão sob diversas condições, conforme as iterações, no contexto do SOC;
• A CONTRATANTE deve definir, em conjunto com a equipe técnica do Banco, casos de uso e procedimentos proativos para atender aos objetivos do SOC, elaborando os respectivos *playbooks*;

• A CONTRATANTE deve apoiar na criação de *playbooks*, que consiste em um manual operacional de segurança com objetivo de fornecer aos envolvidos uma organização e clara compreensão de suas responsabilidades em relação às etapas e procedimentos a serem executados antes, durante e depois de um incidente de segurança, bem como automatizações atendendo ao cenário do respectivo caso de uso;
• A CONTRATANTE deve realizar, para cada caso de uso, no mínimo, as seguintes ações:
o Identificar os requisitos de segurança e conformidade;
o Referenciar a ameaça relacionada;
o Definir as fontes de logs pertinentes;
o Listar os insumos necessários (logs, eventos, dentre outros);
o Criar a lógica das regras;
o Realizar os testes, as regras devem possuir assertividade de no mínimo 90% antes de entrar em produção;
o Realizar ajustes, se necessário;
o Listar produtos gerados (alertas, relatórios, acionamentos, dentre outros);
o Criar procedimentos de tratamento para os cenários de incidentes descritos no caso de uso, ou seja, procedimentos de detecção, resposta e comunicação (*playbooks*);
o Atribuir um nome, incluir breve descrição do contexto e objetivo;
o Categorizar quanto ao contexto do ataque;
o Classificar quanto ao tipo e complexidade;
o Definir os procedimentos de detecção e resposta no SOC;
o Critérios para acionamento hierárquico e funcional;
o Definir plano de comunicação;
o Criar plano de testes e exercício do *playbook*;
o Apoiar a implementação das regras nas ferramentas;
o Mapear o caso de uso na forma de processo e procedimento (BPM);

○ Definir métricas para avaliação dos resultados;
○ Apoiar nas atividades de inclusão, atualização de rotinas, procedimentos (*playbooks*) e/ou configurações junto ao sistema de gestão de incidentes de segurança;
• Faz ainda parte do escopo do serviço especializado de apoio à gestão do SOC, classificar cada caso de uso em nível de complexidade para implementação, considerando os aspectos que envolvem tanto a possibilidade de uso das configurações padrão da ferramenta SIEM como o desenvolvimento de novos processos e ajustes necessários ao ambiente de rede para coleta de informações e também a customização e/ou definição de novos *datasources* e/ou parsers; ○ Baixa complexidade: classificação aplicada para um caso de uso cuja implementação irá utilizar basicamente configurações já existentes no SIEM (dados coletados e disponíveis, envolve um tipo de evento e usa um alerta padrão sem customização); ○ Média complexidade: classificação aplicada para um caso de uso cuja implementação irá requerer que customizações adicionais sejam efetuadas no SIEM (dados coletados e disponíveis, envolve mais de um tipo de evento e sem customização de alertas); ○ Alta complexidade: classificação aplicada para um caso de uso cuja implementação irá requerer customizações no SIEM (dados não disponíveis, exigindo a definição de novos *datasources* e/ou *parsers*, envolve mais de um tipo de evento e há necessidade de customização de alertas);
• Toda atuação nas configurações e ajustes no SIEM, será realizada pela equipe técnica da CONTRATADA;
• Toda atuação nas configurações e ajustes nas ferramentas internas utilizadas pelo Banco será realizada pela equipe técnica do Banco do Nordeste;

- Entram no escopo de atuação do serviço especializado de apoio à gestão do SOC:
  - Simplificar a documentação dos procedimentos e diagramas de fluxos existentes;
  - Revisar e validar os atuais casos de uso e estratégias de resposta elaborados pela CONTRATANTE;
  - Realizar *briefings* e/ou *workshops* para instruir sobre os processos definidos no âmbito do serviço especializado de apoio à gestão do SOC, objetivando proceder com a passagem de conhecimento, desenvolver e manter habilidades específicas de administração do SOC;
  - Realizar *briefings* e/ou *workshops* para instruir sobre a operação do SOC, definição e exercícios dos casos de uso e *playbooks*, apresentar metodologia e funcionamento da estrutura, objetivando desenvolver e manter habilidades pertinentes ao entendimento e atuação das atividades dos níveis, etapas do processo, como detecção e resposta, garantindo assim o alinhamento dos envolvidos com as iniciativas de segurança;
  - Realizar *briefings* e/ou *workshops* sobre tendências, abordagens de ataques e proteções, pertinentes ao contexto de segurança cibernética, objetivando desenvolver e manter habilidades para alavancar a inteligência específica de negócios e de segurança;
  - Fornecer subsídios para a elaboração de conteúdos que apoiem a divulgação das definições e orientações de segurança da informação e segurança cibernética, nas ações de cultura e conscientização viabilizadas através do Portal Intranet, campanhas para os colaboradores e para os clientes, plataformas de ensino a distância, dentre outros;
  - Elaborar conteúdos para até 2 campanhas de conscientização por ano, com temas pertinentes à segurança da informação e/ou segurança cibernética, a serem definidos pelo Banco do Nordeste;
  - Elaborar máteriais para até 2 treinamentos de conscientização aos colaboradores por ano, com temas pertinentes à segurança da informação e/ou segurança cibernética, a serem definidos pelo Banco do Nordeste;
  - Realizar reuniões de alinhamento e entrevistas com colaboradores do Banco (Segurança, TI e Negócio), relevantes ao escopo da atividade, para subsidiar a elaboração das propostas, definição de estratégias e demais entregáveis de maneira a garantir a aplicabilidade ao ambiente do Banco;
  - Manter atualizada toda a documentação e entregáveis, descritos neste serviço especializado de apoio a gestão do SOC;
- A CONTRADA deverá realizar apresentação de relatório mensal com análise de tendências de incidentes de segurança da informação;
- A CONTRADA deverá fornecer um serviço que mapeia os resultados da avaliação para o *Framework* MITRE ATT&CK, permitindo a visualização da cobertura de ameaças e a priorização da mitigação de lacunas;
- A CONTRADA deverá fornecer um serviço de avaliação e relatório do nível de proteção contra ameaças proporcionado pelos controles de segurança. Este serviço deve incluir a identificação de vulnerabilidades e a avaliação da eficácia dos controles de segurança existentes;
- A CONTRADA deverá fornecer um serviço de consultoria para fornecer conselhos adequados sobre detecção de ameaças para incidentes não detectados. Este serviço deve incluir a análise de ameaças potenciais e a recomendação de medidas de detecção;
- A CONTRADA deverá fornecer um serviço de consultoria para fornecer conselhos de mitigação para brechas de segurança identificadas. Este serviço deve incluir a análise de incidentes de segurança e a recomendação de medidas de mitigação;
- A CONTRADA deverá realizar reuniões mensais gerenciais para avaliação e acompanhamento dos serviços contratados.

2.6 TREINAMENTOS – (ITEM 6)

- A CONTRATADA deve prover capacitação técnica na solução ofertada. A capacitação técnica nas disciplinas abaixo descritas deverá contemplar turmas fechadas, com no máximo 15 (quinze) participantes em cada uma delas, a ser realizada sob demanda, considerando a duração mínima conforme descrito abaixo:
  - Solução Integrada de SOC (mínimo de 20 horas, respeitando o limite de 4 (quatro) horas por dia);
  - *Security Analytics* (mínimo de 20 horas, respeitando o limite de 4 (quatro) horas por dia);
  - Tratamento e Resposta a Incidentes de Segurança (mínimo de 20 horas, respeitando o limite de 4 (quatro) horas por dia);
- O treinamento deverá ser ministrado pelo próprio contratado, fabricante ou centro educacional autorizado pelo fabricante;
- O instrutor deverá estar capacitado e habilitado pelo fabricante para a realização do treinamento;
- A capacitação técnica provida deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente do Banco do Nordeste, abrangendo, no mínimo, os seguintes tópicos:
- **Módulo 1 – Solução Integrada de SOC (4 turmas)**:
  - **Introdução**: Conceitos de SIEM, SOAR, UEBA, ASM e análise em segurança, funcionamento da solução e características do produto. Descrição das funcionalidades e navegação em cada módulo da ferramenta e seus modos de funcionamento;
  - **Fontes de dados**: Definição da lista de tipos de dados que o SIEM consome, formas de coletas de dados (Syslog, Flow, SNMP, etc.), ações que podem ser realizadas nos dados adquiridos, integração e configuração de novas fontes de dados à ferramenta de SIEM;
  - **Dashboards**: Descrição das funcionalidades, navegação, criação e customização de dashboards. Análise, busca de dados e definição de incidentes utilizando dashboards;
  - **Relatórios**: Criação, customização, geração e agendamento de relatórios. Funções de filtragem de eventos e construção de métricas para relatórios;
  - **Análise de dados**: Descrição das funcionalidades da ferramenta para análise, investigação, qualificação de dados e alarmes. Definição de buscas e monitoramento de eventos suspeitos, uso de gráficos e filtros avançados para pesquisas de ameaças;
  - **Regras de correlacionamento**: Definição, desenvolvimento, otimização e customização de regras para detectar ataques ou violações de políticas. Conceitos e configurações para redução de falsos positivos;
  - **Automação:** Descrição das funcionalidades e novas tendências de automação e inteligência artificial nas soluções de segurança;
  - **Funções administrativas básicas**: Visão geral das configurações da ferramenta e de perfis de acesso, visão geral de monitoramento da ferramenta e solução de problemas, configurações de segurança e de logs de auditoria do SIEM;

- **Módulo 2 – Security Analytics (4 turmas)**:
  - **Introdução**: Conceitos de segurança, noções de redes, cenário atual de ameaças, principais atacantes e suas metas, técnicas tradicionais de ataque, principais conceitos de *Security Operations Center* (SOC), conceitos de *Threat Intelligence*;
  - **Arquiteturas de segurança**: *Frameworks* e arquiteturas de segurança, defesa de perímetro, segmentação de redes focada em segurança, defesa orientada a detecção;
  - **Ferramentas de Segurança**: Conceitos, aplicações e implementação de *Firewalls* de rede, *Next Generation Firewalls*, *Network Intrusion Prevention System*, *Web Application Firewall*, *HTTP Proxies* e *Web Content Filtering*. Conceitos de *Honeypots/Honeynets*, *Malware Sandbox* e *SSL Decryption*. Conceitos e implementação de SIEM. Varredura de vulnerabilidades e descoberta de host, portas e serviços;
  - **Monitoração de segurança de rede**: Conceitos e arquiteturas de *Network Security Monitoring* (NSM), metodologias de análise. Monitoração utilizando *Network Intrusion Prevention System*. Monitoração utilizando dados de *Firewall*. Entendendo as fontes de dados para NSM: captura de pacotes, *flow* de rede, alertas de ferramentas de segurança, dados estatísticos e correlação, logs de DHCP e DNS. Questões práticas da NSM: rastreando transferência de arquivos, *Service-Side and Client-Side Exploits*, identificando tráfego de *Command and Control* (C&C), análise de tráfego criptografado. Monitoração da situação de segurança do ambiente, aplicações e serviços;
  - **Análise de segurança**: Detecção de ameaças: *botnets*, *malwares*, *ransonware*, etc. Análise de vetores de ameaça, detecção de movimento lateral de ataque, *cyber Kill Chain*. *Behavior Analysis*, análise de log e buscas não estruturadas para detecção de ameaças, qualificação de logs e eventos de interesse. Processos de investigação e construção de casos, contenção de incidentes;
- **Módulo 3 – Tratamento de incidentes de segurança (4 turmas)**:
  - **Introdução**: Conceitos de tratamentos de incidentes de segurança, estrutura de ataque e defesa, visão geral do modulo de GESTÃO DE OPERAÇÕES DE SEGURANÇA, demonstração dos procedimentos necessários para gestão dos incidentes de segurança na ferramenta, práticas recomendadas de tratamento e resposta a incidentes, padrões, estruturas de segurança cibernética, leis, atos e regulamentos;
  - **Processo de tratamento e resposta a incidentes**: Ciclo de vida do incidente contemplando todas as etapas como o planejamento, registro e atribuição, triagem, notificação, contenção, coleta de evidências e análise forense, erradicação, recuperação e atividades pós-incidentes
  - **Lidando e respondendo a diferentes tipos de incidentes de segurança cibernética de forma sistemática**: Abordar o tratamento de incidentes para tipos especificos de incidentes como incidente de *malwares*, incidente de segurança de e-mail, incidente de segurança de rede, incidente de segurança de aplicativo *web*, incidente de segurança de *endpoint*, incidente de segurança de nuvem e incidentes relacionados a ameaças internas.
- Os treinamentos devem ser ministrados nas dependências do Banco do Nordeste, no Centro Administrativo Presidente Getúlio Vargas – CAPGV, localizado na Av. Dr. Silas Munguba, 5700, Passaré, em Fortaleza-CE, em datas e horários definidos posteriormente pelo Banco. O Banco poderá, a qualquer momento, avaliar a possibilidade e optar pelo treinamento na modalidade online, devendo a CONTRATADA moldar o(s) treinamento(s) para tal;
- Caso o treinamento seja realizado na modalidade online, o mesmo deverá ser gravado e enviado ao Banco do Nordestes;

- As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, etc.) serão de exclusiva responsabilidade da CONTRATADA;
- A CONTRATADA deverá fornecer, também em meio digital, o material didático de acompanhamento detalhado, original do fabricante quando aplicável, preferencialmente em português, contendo todos os assuntos abordados na capacitação. Entende-se como material didático, apostilas, slides de apresentações, manuais, livros textos, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em português (Brasil) do material original do fabricante, será aceito material em inglês;
- As turmas deverão ser realizadas no horário compreendido entre 08:30 e 12:30 ou entre 13:30 e 17:30 horas, de segunda a sexta-feira, em turno parcial;
- As apostilas ou manuais impressos deverão ser oferecidos em quantidade idêntica ao número de treinandos de cada turma, com conteúdo oficial do fabricante e atualizado, de acordo com a versão da solução a ser ministrada;
- O Banco do Nordeste reserva-se o direito de realizar a validação técnica e pedagógica do material didático, podendo vir a solicitar à CONTRATADA eventuais correções ou adequações;
- Ao término de cada turma, será realizada uma Avaliação de Reação tendo em vista a medição e avaliação da qualidade da capacitação. O Banco do Nordeste aplicará a Avaliação de Reação em todos os treinandos, com o objetivo de avaliar a satisfação com a capacitação;
- Caso a CONTRATADA, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão do Banco do Nordeste, ela poderá utilizar o seu próprio formulário, porém o mesmo não será utilizado para aprovação da capacitação por parte do Banco do Nordeste;
- Quatro fatores serão objeto de avaliação pelo formulário, conforme descrito abaixo:
    - **Instrutoria** - Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto à sua habilidade didático-pedagógica e de interação com a turma;
    - **Material Didático** - Avalia a percepção dos participantes sobre a adequação e clareza do material didático utilizado na capacitação;
    - **Conteúdo Programático** - Avalia a percepção dos treinandos quanto ao equilíbrio entre teoria e prática, nível de profundidade, exemplos de exercícios, aderência e aplicabilidade;
    - **Autoavaliação** - Avalia a percepção dos participantes quanto a aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado;
- Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio da utilização de quatro conceitos, quais sejam: Fraco (0), Regular (1), Bom (2), e Excelente (3);
- A capacitação técnica provida pela CONTRATADA será submetida à aprovação por parte do Banco do Nordeste;
- O resultado da capacitação será considerado INSATISFATÓRIO quando pelo menos uma das situações abaixo ocorrer:
    - Média final da turma igual ou inferior ao conceito regular (1), excluindo-se o fator Autoavaliação;
    - Média do fator Instrutoria igual ou inferior ao conceito regular (1);

• A CONTRATADA será obrigada a realizar, sem ônus para o Banco do Nordeste, nova capacitação para todas as turmas em que ficar configurado como resultado INSATISFATÓRIO. A critério do Banco do Nordeste, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados. A nova capacitação deverá acontecer segundo um novo calendário a ser definido pelo Banco do Nordeste;
• Após a conclusão da capacitação, mediante solicitação formal do Banco do Nordeste, a CONTRATADA deverá fornecer cópia da apresentação utilizada em mídia eletrônica (CD, DVD ou PENDRIVE), em formatos padrão de mercado (PDF, DOC, PPT ou HTML);
• O Banco do Nordeste se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes, para realizar capacitações internas de seus empregados;
• A CONTRATADA deverá disponibilizar para os participantes que obtiverem no mínimo 75% de frequência, os certificados de conclusão de curso, em meio eletrônico, ao final de cada turma. Aqueles que apresentarem percentuais inferiores não deverão recebê-lo;
• A CONTRATADA deverá enviar ao Banco do Nordeste a lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos, por meio de suas assinaturas em cada dia da capacitação. Em treinamentos de jornada integral, o participante deverá assinar a lista de presença nos dois turnos;
• Para fins de comprovação dos serviços prestados, visando o faturamento, a CONTRATADA deverá encaminhar ao Banco do Nordeste, em até 5 (cinco) dias úteis após o encerramento de cada turma, os certificados e o documento de presença digitalizados.