ANEXO II

ESPECIFICAÇÕES DOS SERVIÇOS

1. FINALIDADE

Este anexo tem por objetivo detalhar os serviços a serem contratados.

2. CONSIDERAÇÕES GERAIS

2.1. A atividade de detecção e registro inicial de Incidentes e Requisições de Serviço deverá ser realizada, em regra, pelos usuários de tecnologia da informação e pela Central de Orientação ao Cliente Interno (Central de Serviço).

2.2. O CONTRATANTE classifica os Incidentes e as Requisições de Serviço para tratamento por nível de criticidade, não podendo ter sua prioridade alterada pelo CONTRATADO, sendo definida como:

2.2.1. **Prioridade Crítica**: Para Incidentes que afetam de forma crítica[1] os serviços de Segurança e TI do CONTRATANTE, causando impacto ao negócio com necessidade de atuação imediata, ou Requisições de Serviços classificadas como prioritárias;

2.2.2. **Prioridade Alta**: para Incidentes que afetam os serviços de Segurança e TI do CONTRATANTE, causando impactos significativos em seu desempenho, existindo ou não a parada dos serviços, ou Requisições de Serviços de alto impacto;

2.2.3. **Prioridade Média**: para Incidentes que não causam impacto significativo sobre a produtividade ou disponibilidade dos serviços de Segurança e TI, porém há a degradação de desempenho dos serviços para os usuários, ou Requisições de Serviços com prazo de atendimento definidos pelos seus respectivos processos;

2.2.4. **Prioridade Baixa**: para Incidentes com impacto mínimo sobre a disponibilidade dos serviços de Segurança e TI, ou Requisições de Serviços que não se enquadram nos critérios de classificação Alta e Média.

2.3. As prioridades poderão ser alteradas pelo CONTRATANTE para classificar os Incidentes e Requisições de Serviços conforme sua necessidade.

2.4. A classificação inicial em relação à prioridade será realizada de acordo com o impacto e a urgência dos Incidentes e Requisições de Serviço ou manualmente e de acordo com matrizes de prioridades disponibilizadas pelo CONTRATANTE.

2.5. O atendimento aos Incidentes classificados com prioridade Alta não poderá ser interrompido até a recuperação do funcionamento dos serviços e aplicações envolvidas.

2.6. O prazo de atendimento se inicia no momento (data/hora/minuto) em que a demanda é aberta e será considerada concluída após o registro da solução da demanda.

[1] Os critérios de prioridade e criticidade para os serviços de segurança são definidos pelo CONTRATANTE.

2.7. O CONTRATANTE se reserva no direito de realizar a avaliação da satisfação do cliente/usuário, através da aplicação de pesquisa de satisfação, por intermédio de consulta aos solicitantes.

2.8. Nos casos em que o CONTRATANTE não considerar satisfatório o resultado do atendimento dos Incidentes e Requisições de serviços, estes poderão ser RECUSADOS e o CONTRATADO deverá executar todos os procedimentos necessários para seu aceite definitivo, registrando posteriormente novas informações e data de conclusão, que passarão por nova validação do solicitante. As correções dos Incidentes e Requisições de serviços serão realizadas sem ônus para o CONTRATANTE e será considerada a última data de conclusão registrada para cálculo de prazos.

2.9. O CONTRATADO deverá elaborar relatórios gerenciais diários e/ou mensais, apresentando-os ao CONTRATANTE até o 5° (quinto) dia útil de cada mês (para os relatórios mensais), ou quando solicitado pelo CONTRATANTE, constando, dentre outras informações, os indicadores e as metas de níveis de serviços acordados e alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período, gráficos de tendências (quantitativas e qualitativas) dos atendimentos, estatísticas de disponibilidades dos serviços, além de qualquer outra informação relevante para a gestão contratual e acompanhamento dos serviços. Fica a critério do CONTRATANTE solicitar alterações nos relatórios acima citados, além de pedir inclusão de novos relatórios.

2.10. As resoluções de Incidentes e o atendimento de Requisições de Serviço deverão ensejar a elaboração de documento(s) formatado(s), de acordo com os padrões definidos pelo CONTRATANTE, de forma que permita aplicar a mesma solução a futuras demandas semelhantes, sendo tais documentos submetidos para a publicação na Base de Conhecimento.

2.11. O CONTRATANTE poderá solicitar, sem ônus adicional, correção dos documentos que não estiverem de acordo com os padrões desejados ou que não corresponderem, na prática, aos procedimentos adotados.

3. MODELO DE EXECUÇÃO E FORMA DE PAGAMENTO

3.1. Para a execução do contrato, será implantado método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o CONTRATANTE como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos produtos e serviços entregues e o CONTRATADO como responsável pela execução dos serviços e gestão dos recursos humanos e físicos necessários. Nesse contexto, o valor mensal a ser pago estará associado ao alcance de metas estabelecidas para a prestação do serviço.

3.2. A natureza dos serviços requer o atendimento tempestivo às demandas dos usuários, muitas das quais não podem ser previamente planejadas por decorrerem de falhas ou dúvidas quanto ao funcionamento das soluções de Segurança e de TI do CONTRATANTE. Por esse motivo, será exigido do CONTRATADO a disponibilidade permanente de equipes qualificadas e dimensionadas de forma compatível com a demanda esperada.

3.3. Todos os serviços objeto desta contratação serão quantificados e demandados através de Ordens de Serviço (OS), conforme descrita adiante.

3.4. A Ordem de Serviço é composta por Unidade de Serviço – US, que é a unidade básica para mensuração dos serviços contratados, sendo equivalente a 01(um) homem/hora.

3.5. Cada serviço poderá ter um conjunto de demandas pré-determinadas e tabeladas, mediante justificativa, contendo tanto suas quantidades de US, quanto seus prazos para execução e finalização;

3.6. O pagamento fica condicionado à realização dos serviços efetivamente prestados pela CONTRATADA, observando a quantidade prevista na Ordem de Serviço.

3.7. A remuneração máxima é estabelecida com base na disponibilidade esperada do serviço, porém os valores efetivamente pagos serão calculados em função do cumprimento de metas de desempenho e qualidade associadas aos serviços.

3.8. Não há previsão de bônus ou pagamentos adicionais para os casos em que o CONTRATADO superar as metas previstas, ou caso seja necessária a alocação de maior número de profissionais para o alcance das metas. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período, bem como o não atendimento da mesma meta em outro período.

4. NIVEL DE SERVIÇO

Os níveis de serviços de todos os itens da contratação estão descritos no **Anexo III - Níveis Mínimos de Serviços.**

5. PERFIS DOS PROFISSIONAIS

5.1. O CONTRATADO deverá organizar-se considerando a existência dos seguintes papéis, não se limitando a estes, caso considere a necessidade de outros papéis que julgue apropriados para o bom desempenho das atividades contratadas:

5.1.1. **Supervisor Técnico** (responsável pelo gerenciamento da execução dos serviços e supervisão técnica do Contrato);

5.1.2. **Líder Técnico** (responsável pelo gerenciamento da execução das atividades do serviço da contratação e liderança das equipes técnicas especialistas);

5.1.3. **Equipe Técnica Especialista** (responsável pela execução das atividades do serviço da contratação);

5.1.4. **Equipe de Consultoria e Projeto** (responsáveis por apoiar nos projetos relacionados à Segurança Corporativa**).**

5.2. Os Perfis dos Profissionais de todos os itens da contratação estão descritos no **Anexo IV - Perfis e Qualificações dos Profissionais do Contratado.**

6. VOLUME ESTIMADO

6.1. O volume inicial dos serviços está descrito no **Anexo V – Volume Estimado dos Serviços.**

7. LOCAL DE PRESTAÇÃO DOS SERVIÇOS

7.1. Todas as atividades serão executadas nas dependências do CONTRATANTE, a saber:

7.1.1. Site Principal (Direção Geral) situado na Av. Dr. Silas Munguba, 5.700, em Fortaleza-CE;

7.2. Os profissionais do CONTRATADO sempre deverão exercer suas atribuições sob a supervisão técnica e administrativa de preposto responsável pela realização dos serviços contratados.

7.3. O CONTRATANTE poderá, a qualquer tempo, avaliar a possibilidade de atuação remota de uma ou mais unidades de serviços envolvidos no objeto do contrato.

7.4. Durante a execução do contrato, de acordo com as necessidades que venham a surgir e visando à excelência na prestação de serviços de suporte aos negócios da instituição, o Banco poderá, a qualquer tempo, em comum acordo com o contratado e desde que não haja alteração nos valores dos serviços contratados, solicitar a atuação remota de profissionais previstos para atuação presencial, bem como a atuação presencial de profissionais com atuação remota previamente definida.

7.5. O CONTRATANTE não custeará deslocamento de equipe para suas instalações, cabendo ao CONTRATADO a responsabilidade pelo deslocamento dos profissionais envolvidos na prestação dos serviços de suas instalações para as instalações do CONTRATANTE, inclusive quanto às demais despesas de passagem, hospedagem, alimentação etc.

8. PROVIMENTO DE RECURSOS (INSTALAÇÕES, FERRAMENTAS DE TRABALHO ETC.) PARA REALIZAÇÃO DOS SERVIÇOS

8.1. Será responsabilidade do CONTRATANTE o ônus com o estabelecimento das condições para execução das atividades em suas dependências, abrangendo infraestrutura de *hardware* (equipamentos) e *software* (ferramentas de trabalho), excetuando-se despesas de passagem, hospedagem, alimentação etc.

8.2. O CONTRATADO deverá implementar sistemática de acompanhamento e supervisão dos serviços sob sua responsabilidade, em níveis operacionais, para que, dentre outras finalidades, possa fornecer informações ao CONTRATANTE.

8.2.1. Os níveis de serviços devem ser apresentados mensalmente, até o 5º (quinto) dia útil do mês subsequente ao da prestação dos serviços, pelo CONTRATADO para validação e autorização de pagamento.

8.2.2. Em qualquer momento da execução de um serviço pelo CONTRATADO, o CONTRATANTE poderá solicitar informações a respeito da execução do serviço cujo relatório de resposta deverá ser entregue ao CONTRATANTE pelo CONTRATADO, em no máximo 5 (cinco) dias úteis.

8.2.3. As informações a serem fornecidas dizem respeito ao andamento dos serviços no momento da solicitação, comparações com períodos anteriores, estimativas de término, modificações em escopo e prazo, se for o caso.

8.2.4. Durante o período de execução do Contrato, o CONTRATANTE, a seu critério, poderá agendar reuniões para planejamento, organização e avaliação da prestação dos serviços com o CONTRATADO, a serem realizadas em seu site principal em Fortaleza-CE.

9. OBRIGAÇÕES DO CONTRATADO

Caberá ao CONTRATADO o cumprimento das seguintes obrigações, além daquelas específicas, contidas no Contrato, no Edital e seus Anexos:

9.1. Efetuar a entrega dos serviços de acordo com o estabelecido nos anexos do Edital e totalmente aderentes aos produtos e tecnologias utilizados pelo CONTRATANTE;

9.1.1. O CONTRATANTE pode, a qualquer tempo, atualizar os produtos e tecnologias utilizados comprometendo-se o CONTRATADO a adaptar-se em um prazo máximo de 60 (sessenta) dias corridos, a partir da data de notificação por parte do CONTRATANTE;

9.2. Formalizar a indicação de prepostos/coordenadores da empresa e substituto eventual para o Supervisor de Execução do Contrato;

9.3. Gerenciar os recursos humanos utilizados na execução dos serviços contratados pelo CONTRATANTE, realizando as atividades relativas ao repasse de informações, acompanhamento e supervisão dos serviços;

9.4. recrutar e selecionar os colaboradores necessários à realização dos serviços, de acordo com o disposto nas Qualificações Exigidas de cada perfil profissional, **Anexo IV - Perfis e Qualificações dos Profissionais do Contratado**;

9.5. Manter e disponibilizar ao CONTRATANTE documentação comprobatória da qualificação dos profissionais alocados na execução dos serviços e disponibilizar essa documentação ao CONTRATANTE, sempre que solicitada;

9.6. Assegurar que a remuneração do contratado, em sua totalidade, deverá ser estabelecida unicamente através de Contrato individual de Trabalho conforme a CLT, não sendo permitida a modalidade de regime de trabalho PJ (Pessoa Jurídica);

9.7. Todos os profissionais alocados na prestação dos serviços deverão possuir perfil técnico e profissional adequado ao escopo do serviço a ser realizado, devendo ser continuamente treinados e avaliados para assegurar o bom desempenho de suas atribuições além de contribuir para o processo de melhoria contínua, visando a evolução profissional dos mesmos em função das atualizações tecnológicas que venham a acontecer nesses ambientes;

9.8. Ao final de cada período de vigência do contrato, a empresa deverá apresentar uma listagem de todos os profissionais alocados (prestando serviço ao Banco do Nordeste do Brasil) com os respectivos treinamentos e carga horária total no período. Será requerido o mínimo de 40 horas-aula por ano por profissional;

9.9. Assegurar a seus profissionais a concessão dos benefícios obrigatórios e reajustes previstos nos acordos e convenções de trabalho vigentes para as respectivas categorias profissionais;

9.10. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da contratação;

9.11. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os profissionais que prestarão os serviços não manterão nenhum vínculo empregatício com o CONTRATANTE;

9.12. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os profissionais que prestarão os serviços durante a execução do Contrato, ainda que acontecido nas dependências do CONTRATANTE;

9.13. Assumir a responsabilidade por todos os encargos de eventual demanda trabalhista, civil ou penal, relacionada à execução do Contrato, originariamente ou vinculada por prevenção, conexão ou continência;

9.14. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus profissionais que forem acidentados ou acometidos de mal súbito;

9.15. Manter seus profissionais devidamente identificados por meio de crachá, quando em trabalho nas dependências do CONTRATANTE;

9.16. Devolver ao CONTRATANTE os crachás eventualmente fornecidos para acesso a determinados ambientes quando do desligamento do profissional ou do término do Contrato, devendo o CONTRATANTE ser ressarcido por eventuais extravios ou danos;

9.17. Providenciar a imediata substituição de qualquer empregado considerado inadequado à execução dos serviços contratados, mediante solicitação do CONTRATANTE;

9.18. Obedecer ao especificado em todas as normas, padrões, processos e procedimentos do CONTRATANTE, estabelecidos nos Anexos, e respeitar os princípios éticos e compromissos de conduta, definidos no Código de Conduta Ética do CONTRATANTE, enquanto perdurar a relação contratual;

9.18.1. O CONTRATANTE pode, a qualquer tempo, atualizar suas normas, padrões, processos e procedimentos comprometendo-se o CONTRATADO a se adaptar em um prazo máximo de 30 (trinta) dias corridos, a partir da data de notificação por parte do CONTRATANTE;

9.19. Participar, quando convocado, de reuniões para alinhamento de expectativas contratuais com equipe de profissionais do CONTRATANTE;

9.20. Prestar informações e esclarecimentos sobre a execução dos serviços e procedimentos, no âmbito do Contrato, no prazo de 5 (cinco) dias úteis, a contar da data do recebimento da solicitação feita pelo CONTRATANTE;

9.21. Responsabilizar-se pelo transporte, sem ônus para o CONTRATANTE, do seu pessoal até o local de trabalho, inclusive em casos de paralisação dos transportes coletivos, bem como nas situações nas quais se faça necessária a execução dos serviços em regime extraordinário;

9.22. Responder por quaisquer danos causados, por seus profissionais, a bens de propriedade do CONTRATANTE ou de terceiros, quando tenham sido causados durante a execução dos serviços contratados;

9.23. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, serviços efetuados em que se verificarem vícios, defeitos e incorreções, durante a vigência do Contrato;

9.24. Utilizar *softwares* e demais ferramentas de trabalho tornados disponíveis pelo CONTRATANTE para a execução dos serviços, se for o caso;

9.25. Reportar ao CONTRATANTE, quaisquer anormalidades, erros ou irregularidades que possam comprometer a execução dos serviços e o bom andamento das atividades;

9.26. Solicitar ao CONTRATANTE a revisão, modificação ou revogação de privilégios de acesso a sistemas, informações e recursos do CONTRATANTE, quando da transferência, remanejamento, promoção ou demissão de profissional sob sua responsabilidade;

9.27. Disponibilizar, ao CONTRATANTE, toda a informação utilizada e / ou produzida na execução dos serviços prestados, em até 30 (trinta) dias corridos, sem quaisquer ônus adicionais para o CONTRATANTE, contados da data de finalização do Contrato, eliminando de suas bases de informações os documentos encaminhados pelo CONTRATANTE para a especificação dos serviços, bem como outros artefatos decorrentes desta e demais documentações pertinentes;

9.28. Apresentar relação dos empregados que utilizarão férias, com antecedência de 30 (trinta) dias, bem como o nome dos respectivos substitutos, que deverão atender às qualificações técnicas exigidas para a função substituída;

9.29. Informar, em até 02 (dois) dias úteis, a ocorrência de afastamento de empregados, bem como o nome dos respectivos substitutos, que deverão atender às qualificações técnicas exigidas para a função substituída;

9.30. O CONTRATADO deverá elaborar e implantar um Plano de Contingência que consiste na previsão e planejamento de ações que garantam o funcionamento de todas as atividades de atendimento nos dois ambientes, do CONTRATANTE e do CONTRATADO, diante de situações de crise, tais como, greves, ausências prolongadas de funcionários, pandemias, dentre outras;

9.30.1. O Plano de Contingência deverá considerar, no mínimo:

9.30.1.1. as atribuições e a composição de uma Gerência de Crise;

9.30.1.2. a manutenção da execução de, no mínimo, 60% (sessenta por cento) dos serviços de atendimento (demanda e pessoal) com base na média dos últimos 3 (três) meses, conforme os indicadores definidos;

9.30.1.3. a transferência dos serviços prestados nas dependências do CONTRATADO, para outra localidade, na ocorrência de situações de impedimento total para a realização dos serviços, respeitando o perímetro definido neste documento, de forma imediata, sem ônus adicional para o CONTRATANTE;

9.30.1.4. A gerência da crise é uma composição imediata e após identificação de algum incidente que comprometa ou possa comprometer o serviço, devendo ser composta por pessoas com poder de decisão do CONTRATADO.

10. OBRIGAÇÕES DO CONTRATANTE

10.1. Alocar colaboradores para gestão e fiscalização do Contrato.

10.2. Alocar colaboradores para prestar informações sobre os processos e serviços desenvolvidos nas unidades organizacionais da Área de Segurança e TI, com o intuito de fornecer subsídios para a prestação dos serviços pelo CONTRATADO.

10.3. Comunicar, formalmente, ao CONTRATADO quaisquer falhas verificadas no cumprimento do Contrato.

10.4. Disponibilizar, para o CONTRATADO, os recursos de *hardware* e *software* necessários à prestação dos serviços, bem como o suporte necessário ao uso destes recursos, quando executado nas dependências do CONTRATANTE.

10.5. Efetuar o pagamento ao CONTRATADO, mensalmente, considerando os serviços prestados efetivamente "aceitos" pelo CONTRATANTE e os serviços cujas "entregas" já tenham decorrido os respectivos prazos para a emissão dos aceites.

10.6. Fornecer os requisitos de arquitetura tecnológica e demais padrões adotados pela Área de Tecnologia do CONTRATANTE que deverão ser observados pelo CONTRATADO na prestação dos serviços.

10.7. Fornecer crachá de acesso às suas dependências, de uso obrigatório pelos profissionais do CONTRATADO.

10.8. Observar o cumprimento dos requisitos de qualificação profissional exigidos no Termo de Referência e Anexos, solicitando ao CONTRATADO as substituições e os treinamentos que se verificarem necessários.

10.9. Permitir acesso dos profissionais do CONTRATADO às suas dependências.

10.10. Prover equipamentos, *softwares* e sistemas de informação para a execução dos serviços contratados, quando for o caso.

11. QUADRO RESUMO DAS UNIDADES DE SERVIÇO POR PROCESSOS/SERVIÇOS E MACROATIVIDADES

As atividades a serem executadas estão agrupadas em macroatividades, que por sua vez integram um serviço, vinculado a UNIDADE DE SERVIÇO, cujo resumo é apresentado na tabela abaixo e o detalhamento nos itens seguintes:

Unidade de Serviço	Processo/Serviço	Perfil	Macroatividade
US - 1	Serviço de Supervisão Técnica de Segurança da Informação e Cibernética	-	Gestão da Execução do Serviço
			Apoio em Projetos
			Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços
			Gestão de Indicadores
			Gestão de Conhecimento
US - 2	Serviço de Liderança Técnica de Governança de Segurança da Informação	-	Liderar e coordenar as atividades técnicas da equipe de Gerenciamento do Conhecimento
			Apoio às atividades técnicas de Gerenciamento do Conhecimento
			Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços
			Executar Exercícios de simulação
			Apoio em projetos
US - 3	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)	-	Liderar e coordenar as atividades técnicas das equipes de Segurança da Informação e Cibernética (Operações de Segurança I, II e III)
			Apoio às atividades técnicas de Segurança da Informação e Cibernética das equipes de Operações de Segurança I, II e III
			Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços
			Apoio em projetos
US - 4	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)	-	Liderar e coordenar as atividades técnicas das equipes de Segurança da Informação e Cibernética (Operações Defensivas) e Atendimento e Tratamento de Requisições e Resposta a Incidentes
			Apoio às atividades técnicas de Segurança da Informação e Cibernética (Operações Defensivas) e Atendimento e Tratamento de Requisições e Resposta a Incidentes
			Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços
			Apoio em projetos
US - 5	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)	-	Liderar e coordenar as atividades técnicas da equipe de Segurança da Informação e Cibernética (Operações Ofensivas)
			Apoio às atividades técnicas de Segurança da Informação e Cibernética da equipe de Operações Ofensivas
			Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços

			Apoio em projetos
US - 6	Serviço de Suporte ao Gerenciamento de Projetos e Melhorias	-	Liderar e coordenar as atividades técnicas de suporte ao gerenciamento de projetos e melhorias
			Apoio às atividades técnicas relacionadas aos projetos e melhorias
			Suporte às atividades de gerenciamento de projetos e melhorias
			Prospecção, concepção, construção e melhorias dos projetos e dos planos de projetos
US - 7	Serviço de Suporte ao Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)	Perfil I	Elaboração dos Documentos e gerenciamento da Base de Conhecimento
			Prospecção, concepção e construção de padrões, modelos e controles para melhoria dos serviços
			Apoio às atividades de gestão de conhecimento
		Perfil II	Elaboração de campanhas de conscientização
			Elaboração de treinamentos e workshops
			Gerenciamento de maturidade da documentação dos processos / serviços / atividades
		Perfil III	Elaboração de processos e fluxos
			Prospecção, concepção e construção de padrões, modelos e controles para melhoria dos serviços
			Gerenciamento de desempenho dos processos e fluxos
			Apoio as atividades de gestão de conhecimento
US-8	Serviço de Suporte ao Gerenciamento de Dados	-	*Business Intelligence*
			Manipulação de Dados
			Apoio às atividades de gestão de conhecimento
			Criar/manter painéis e dashboards executivos
US - 9	Serviço de Segurança da Informação e Cibernética (Operações de Segurança I)	-	Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições
			Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos
			Apoio em Projetos
US - 10		-	Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições

	Serviço de Segurança da Informação e Cibernética (Operações de Segurança II)		Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos
			Apoio em Projetos
US - 11	Serviço de Segurança da Informação e Cibernética (Operações de Segurança III)	-	Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições
			Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos
			Apoio em Projetos
US - 12	Serviço de Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)	-	Classificação de Incidentes, Problemas e Requisições
			Triagem dos Alertas de Segurança
			Monitoramento, Acompanhamento e Comunicação de Incidentes e Alertas de Segurança
			Investigação, diagnóstico, resolução e encerramento de Requisições de Serviços e de Incidentes de Segurança
US - 13	Serviço de Segurança da Informação e Cibernética (Operações Defensivas)	Perfil I	Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições
			Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos
			Apoio em Projetos
		Perfil II	Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições
			Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos
			Suporte e melhoria dos serviços
			Apoio em Projetos
US - 14	Serviço de Segurança da Informação e Cibernética (Operações Ofensivas)	Perfil I	Análise de vulnerabilidades em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas
			Testes de intrusão em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas
			Exercícios *Red Team* em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas
			Monitoramento, Acompanhamento e Comunicação de Incidentes e Alertas de Segurança
			Apoio em Projetos
		Perfil II	Análise de vulnerabilidades em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas

			Testes de intrusão em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas
			Exercícios *Red Team* em sistemas operacionais, equipamentos e dispositivos de rede, *softwares* e sistemas
			Suporte e melhoria dos serviços
			Apoio em Projetos
US – 15	Serviço de Consultoria	Perfil I	Suporte às atividades de prospecção de Novas Tecnologias de serviços de Segurança da Informação
			Apoio no suporte e melhorias das ferramentas e serviços de segurança da informação utilizadas no Banco do Nordeste
			Estudos de Viabilidade e Análise comparativas
			Análise de Conformidade às Leis, Regulamentações e Normas
			Apoio na definição de Políticas, Procedimentos e Diretrizes
			Elaboração de documentos com as atividades desempenhadas para a base de conhecimento
			Levantamento de melhorias dos processos e modelos de maturidade
			Apoio consultivo à equipe técnica especialista
			Atividades relacionadas à análise Forense
			Apoio na elaboração de Campanhas de Conscientização
			Apoio no desenvolvimento de atividades de treinamento e capacitação sobre a temática de Segurança da Informação
		Perfil II	Desenvolver e suportar as atividades de *Security Development Lifecycle*
			Apoiar nos testes de software para validar as especificações de segurança e/ou vulnerabilidades
			Apoiar na difusão da cultura de Segurança da Informação no desenvolvimento Ágil, promovendo a cultura de *DevSecOps*
			Estudos de Viabilidade e Análise comparativas
			Análise de Conformidade às Leis, Regulamentações e Normas
			Elaboração de documentos com as atividades desempenhadas para a base de conhecimento

			Apoio na definição de Políticas, Procedimentos e Diretrizes
			Apoio consultivo às equipes de desenvolvimento
			Apoio na elaboração de Campanhas de Conscientização
			Apoio no desenvolvimento de atividades de treinamento e capacitação sobre a temática de Desenvolvimento Seguro
US - 16	Serviço de Operações de Combate e Prevenção a Fraude	Perfil I	Monitoramento, triagem e acompanhamento de eventos
		Perfil II	Análise e investigação de eventos
			Operacionalização de sistemas, serviços e recurso tecnológicos utilizados na prevenção e combate a fraudes
			Configuração, manutenção e suporte de sistemas, serviços e recurso tecnológicos utilizados na prevenção e combate a fraudes
			Apoio técnico
		Perfil III	Análise e investigação de eventos
			Suporte e melhoria dos serviços
			Apoio em projetos
US-17	Serviço de Operações de Combate e Prevenção à Lavagem de Dinheiro	Perfil I	*Business Intelligence*
			Manipulação de Dados
			Programação para Análise de Dados
			Suporte às atividades de Análise de Dados
			Apoio em projetos
		Perfil II	Análise de requisitos e modelagem de dados
			Manipulação de Dados
			Gerenciamento de Dados
			Suporte às atividades da Equipe de Dados
			Apoio em projetos

12. ATIVIDADES DAS UNIDADES DE SERVIÇO

12.1. Os quadros abaixo trazem relações básicas, não exaustivas, das atividades que compõem cada serviço/macroatividade, assim como relação de atividades comuns a todas as macroatividades.

12.2. Em função das otimizações, propostas de melhorias dos serviços e/ou novas tecnologias incorporadas/substituídas pelo CONTRATANTE, esta lista poderá sofrer alterações, ao longo da execução contratual, a fim de contemplar as atividades/adequações necessárias à perfeita execução dos serviços sem que se caracterize, necessariamente, alteração, acréscimo ou supressão dos serviços ao objeto contratado.

12.3. **Atividades da US - 1 - Serviço de Supervisão Técnica de Segurança da Informação e Cibernética**

MACROATIVIDADES	ATIVIDADES
Gestão da Execução do Serviço	Gerenciar, supervisionar, liderar, orientar e apoiar tecnicamente as equipes providas pela CONTRATADA;
	Atuar com a equipe de modo a avaliar e reportar ameaças, vulnerabilidades, riscos residuais e estruturar planos de ação;
	Identificar os recursos que exigem medidas de segurança e gerenciar o tema com as áreas envolvidas;
	Definir e documentar estratégias para escalabilidade horizontal e vertical dos recursos, componentes do ambiente, arquitetura e equipe;
	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;
	Zelar pela boa educação e apresentação pessoal dos colaboradores, mantendo a qualidade dos serviços prestados no que tange a presteza, cordialidade, educação, clareza e eficiência, favorecendo as relações interpessoais e ambiente agregador;
	Apoio à implementação e manutenção de procedimentos para garantir a manutenção permanente de segurança em todos os domínios pertinentes ao tema;
	Apoio no programa de conscientização;
	Apoio na execução de exercícios de simulação (*TableTop*).
Apoio em Projetos	Acompanhamento do portfólio de projetos de segurança corporativa e iniciativas;
	Apoio à implementação e manutenção de políticas de segurança, normas e diretrizes para garantir a manutenção permanente da segurança em todos os domínios pertinentes ao tema;
Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços	Gestão e mapeamento dos riscos de Segurança da Informação juntamente com a equipe de consultores e líderes com implantação de programas, controles e políticas, buscando a constante identificação de ações de melhoria para cada serviço.
	Definir e documentar diretrizes para a gestão de incidentes de segurança;
	Definir e documentar estratégias para elaboração do plano de comunicação em crise, e para identificação de pessoas/áreas chave e formalizações;
	Definir e documentar estratégias para melhoria do modelo operacional de segurança cibernética;
	Elaborar boletins periódicos, baseados nas informações de dados globais dos centros de pesquisa de ameaças, contendo novas táticas e técnicas de ataque,

MACROATIVIDADES	ATIVIDADES
	vulnerabilidades e mecanismos de proteção de interesse do Banco do Nordeste;
	Recomendar e coordenar a implementação de controles técnicos para apoiar e aplicar políticas de segurança definidas;
	Manter atualizada e divulgar para o CONTRATANTE a documentação dos processos e seus anexos. A divulgação deve ser realizada semestralmente ou por solicitação do CONTRATANTE.
Gestão de Indicadores	Assegurar a apuração dos indicadores de níveis de serviço alcançados por todos os processos pertencentes ao escopo do contrato, promovendo alinhamento constante com os responsáveis pelos processos por parte do CONTRATANTE, buscando a constante identificação de ações de melhoria para cada processo.
	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);
	Elaborar e apresentar, mensalmente, relatório gerencial dos indicadores apurados para todos os serviços pertencentes ao escopo do contrato, apresentando dificuldades, oportunidades de melhoria, bem como demais informações necessárias para a evolução do contrato em questão.
Gestão de Conhecimento	Definir o plano de treinamento inicial e contínuo dos profissionais contratados para execução dos serviços;
	Realizar oficinas de transferência de conhecimento acerca das diversas atividades realizadas pelos profissionais do CONTRATADO dentro do escopo dos processos contratados.
	Promover ações de capacitação e conscientização sobre segurança da informação.

12.4. Atividades da US - 2 - Serviço de Liderança de Governança de Segurança da Informação

MACROATIVIDADES	ATIVIDADES
Liderar e coordenar as atividades técnicas das equipes de Gerenciamento do Conhecimento e Dados	Coordenar e liderar as atividades técnicas dos serviços de Gerenciamento do Conhecimento e Dados;
	Coordenar a Padronização de Documentos para Base de Conhecimento, Modelo de Maturidade, Processos do Grupos de Resposta a Incidentes de Segurança e dos Processos das demais unidades de serviços do contrato;
	Realizar estratégia de disseminação de treinamentos e campanhas de conscientização;
	Realizar o planejamento das entregas de tarefas definindo prazos e estratégias de priorização;
	Acompanhar a qualidade dos painéis, *dashboards*, relatórios e formulários criados pela equipe de Gerenciamento de Dados;
	Acompanhar a avaliação dos modelos de maturidade e postura de segurança da organização;
	Acompanhar a execução dos planos de ações recomendados após as avaliações de desempenho e maturidades;
	Acompanhar e monitorar as entregas e os indicadores de qualidade dos serviços;

	Responsabilizar-se pela qualidade no registro das informações detalhadas na Base de Conhecimento como solução de contorno, erro conhecido, documentos de construção e teste, solução definitiva, dentre outros.
Apoio as atividades técnicas das equipes de Gerenciamento do Conhecimento e Dados	Apoiar a equipe na Criação, Edição e Manutenção de Documentos da Base de Conhecimento, Modelo de Maturidade, Processos do Grupo de Resposta a Incidentes de Segurança e dos Processos das demais unidades de serviços do contrato;
	Mapear processos, fluxos e procedimentos das unidades de serviço do contrato;
	Definir e documentar modelo simplificado para documentação de procedimentos e diagramas de fluxos;
	Aprovar os documentos de conhecimento para publicação na Base de Conhecimento.
	Indicar qual a categorização do documento.
	Encaminhar os documentos de conhecimento válidos e ajustados para aprovação da gestão.
	Gerar informações gerenciais sobre o respectivo processo.
	Sugerir Principais Indicadores de Desempenho (KPIs).
	Sugerir criação de painéis e *dashboards* técnicos e gerenciais;
	Sugerir criação de *bots* para disseminar informações sobre a temática de segurança da informação;
	Coordenar o desenvolvimento de treinamentos de *Onboarding* para novos colaboradores e treinamento de Reciclagem de Conhecimentos para os demais colaboradores do contrato;
	Coordenar o desenvolvimento de atividades de treinamento e capacitação sobre a temática de Segurança da Informação e as demais unidades de serviços do contrato
	Coordenar o programa de conscientização e a elaboração de Campanhas de Conscientização;
	Criar boletim informativo sobre os resultados das campanhas e realizar apresentação gerencial dos resultados periodicamente.
Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços	Elaboração de documentos com processo e atividades desempenhadas pelas equipes para a base de conhecimento;
	Definir e documentar estratégias para melhoria das operações de Gerenciamento do Conhecimento e Dados.
	Coordenar a implementação de controles técnicos para apoiar as operações de Gerenciamento do Conhecimento e Dados.
Executar Exercícios de simulação	Coordenar a execução de exercícios de simulação (*TableTop*) com apoio do Supervisor e demais líderes de equipes;
	Elaborar todo o planejamento, cronograma e artefatos necessários para execução dos exercícios;
	Elaborar relatórios de resultados e plano de ações para melhorias dos serviços e equipes com apoio do supervisor e demais líderes;
	Acompanhar a execução dos planos de ações recomendados após o exercício de simulação.
Apoio em projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços sob responsabilidade do Grupo de Resposta a Incidentes de Segurança.

12.5. Atividades da US - 3 - Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)

MACROATIVIDADES	ATIVIDADES
Liderar e coordenar as atividades técnicas das equipes de Segurança da Informação e Cibernética (Operações de Segurança I, II e III)	Coordenar e liderar as atividades técnicas dos serviços das equipes de Segurança da Informação e Cibernética (Operações de Segurança I, II e III);
	Orientar sobre o uso de fontes de inteligência de ameaças contextualizadas (*ThreatIntelligence*), e uso da abordagem de caça (*ThreatHunting*);
	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 estratégias de segurança para uso de serviços e soluções em nuvem;
	Realizar o planejamento de atividades definindo prazos e estratégias de priorização;
	Acompanhar e monitorar as entregas e os indicadores de qualidade do serviço;
Apoio às atividades técnicas de Segurança da Informação e Cibernética das equipes de Operações de Segurança I, II e III	Apoiar as equipes no tratamento, investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	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;
	Elaborar *baseline* de configuração das soluções sob responsabilidade das equipes de operações de segurança I, II e III (SIEM, DLP, O365, CASB, HSM e GIA) e mantê-las atualizadas conforme cada atualização de versão;
	Realizar avaliação de *healthcheck* periódico nas soluções sob responsabilidade das equipes de operações de segurança I, II e III (SIEM, DLP, O365, CASB, HSM e GIA), avaliar os resultados e apresentar apontamentos e recomendações;
	Apoiar as equipes no planejamento, coordenação de atividades e execução das mudanças;
	Auxiliar a equipe técnica na elaboração do documento de Requisição de Mudança (RDM)
	Negociar a janela de implantação com a equipe responsável no Ambiente de Operação de TI;
	Acompanhar a solicitação, planejamento, implantação, teste de conformidade e encerramento de RDMs;
	Elaborar 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;
	Elaboração de relatórios técnicos e gerenciais;
Prospecção, concepção e construção de fluxos e controles para	Elaboração de documentos com processo e atividades desempenhadas pela equipe para a base de conhecimento;
	Definir e documentar estratégias para melhoria das operações de Segurança da Informação e Cibernética das equipes de Operações de Segurança I, II e III;

MACROATIVIDADES	ATIVIDADES
melhoria dos serviços	Coordenar a implementação de controles técnicos para apoiar as operações de Segurança da Informação e Cibernética das equipes de Operações de Segurança I, II e III;
	Desenvolver e documentar estratégias para o gerenciamento de segurança da informação e eventos (SIEM), contemplando atividades de registro, lógica para correlações, monitoramento e alertas;
Apoio em projetos	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Acompanhamento e revisão das políticas de segurança que envolvem as soluções e serviços sob responsabilidade das equipes de operações de segurança I, II e III;
	Apoio no programa de conscientização;
	Apoio na execução de exercícios de simulação (*TableTop*).

12.6. Atividades da US - 4 – Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)

MACROATIVIDADES	ATIVIDADES
Liderar e coordenar as atividades técnicas das equipes de Segurança da Informação e Cibernética (Operações Defensivas) e Atendimento e Tratamento de Requisições e Resposta a Incidentes	Coordenar e liderar as atividades técnicas dos serviços das equipes de Segurança da Informação e Cibernética (Operações Defensivas) e Atendimento e Tratamento de Requisições e Resposta a Incidentes;
	Gerenciamento das atividades do *Security Operations Center* coordenando a classificação e priorização dos eventos;
	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;
	Gestão das vulnerabilidades e articulação para as priorizações e correções;
	Elaborar *baseline* de configuração das soluções sob responsabilidade das equipes de operações defensivas e mantê-las atualizadas conforme cada atualização de versão;
	Realizar avaliação de *healthcheck* periódico nas soluções sob responsabilidade das equipes de operações defensivas, avaliar os resultados e apresentar apontamentos e recomendações;
	Realizar o planejamento de atividades definindo prazos e estratégias de priorização;
	Definir e documentar metodologia de criação e de gerenciamento de métricas e indicadores de desempenho;
	Acompanhar e monitorar as entregas e os indicadores de qualidade do serviço;
Apoio às atividades técnicas de Segurança da Informação e Cibernética	Apoiar a equipe no tratamento, investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	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;

MACROATIVIDADES	ATIVIDADES
(Operações Defensivas) e Atendimento e Tratamento de Requisições e Resposta a Incidentes	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;
	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;
	Apoio no planejamento, coordenação de atividades e execução das mudanças;
	Auxiliar a equipe técnica na elaboração do documento de Requisição de Mudança (RDM);
	Negociar janela de implantação com equipe responsável no Ambiente de Operação de TI;
	Acompanhar a solicitação, planejamento, implantação, teste de conformidade e encerramento de RDMs;
	Elaborar 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;
	Elaboração de relatórios técnicos e gerenciais;
Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços	Elaboração de documentos com processo e atividades desempenhadas pela equipe para a base de conhecimento;
	Definir e documentar estratégias para melhoria das operações de Segurança da Informação e Cibernética das equipes de Operações Defensivas e *Security Operations Center*
	Elaborar manual de operações do SOC, descrevendo: diretrizes, processos e procedimentos sobre o funcionamento e controles da estrutura;
	Padronização dos procedimentos de resposta a incidentes, os procedimentos devem conter as melhores práticas para o tratamento e contenção dos incidentes, de modo que viabilize a execução das medidas corretivas necessárias pelo Banco do Nordeste. Esses procedimentos devem ser orientados para incidentes aplicáveis a ambientes genéricos ou que constem da base de conhecimento do CONTRATADO;
	Revisar e validar os atuais casos de uso e estratégias de resposta elaborados pelo CONTRATANTE;
	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.
	Coordenar as atividades de melhoria e evolução da maturidade dos serviços
Apoio em projetos	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Acompanhamento e revisão das políticas de segurança que envolvem as soluções e serviços sob responsabilidade das equipes de Operação Defensivas e Atendimento e Tratamento de Requisições e Resposta a Incidentes;
	Apoio no programa de conscientização;
	Apoio na execução de exercícios de simulação (*TableTop*).

12.7. Atividades da US - 5 - Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)

MACROATIVIDADES	ATIVIDADES
Liderar e coordenar as atividades	Coordenar e liderar as atividades técnicas dos serviços da equipe de Segurança da Informação e Cibernética (Operações Ofensivas);

MACROATIVIDADES	ATIVIDADES
técnicas da equipe de Segurança da Informação e Cibernética (Operações Ofensivas)	Gestão das vulnerabilidades e articulação para as priorizações e correções;
	Realizar o planejamento de atividades, definindo prazos e estratégias de priorização;
	Acompanhar e monitorar as entregas e os indicadores de qualidade do serviço;
Apoio as atividades técnicas de Segurança da Informação e Cibernética da equipe de Operações Ofensivas	Apoiar a equipe no tratamento, investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Apoio no planejamento, coordenação de atividades e execução das mudanças;
	Auxiliar equipe técnica na elaboração de planos de teste;
	Solicitar ambiente e credenciais para os testes;
	Negociar janela de teste com equipe responsável dos outros ambientes;
	Acompanhar a solicitação, planejamento, execução e encerramento dos testes;
	Elaborar planos de exercício de *Red Team*;
	Avaliar resultados e evolução dos exercícios de *Red Team* e propor melhorias nas futuras execuções;
	Realizar recomendações de segurança para manter um ambiente seguro baseado nos resultados obtidos do exercício de *Red Team*;
	Elaborar 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;
	Elaboração de relatórios técnicos e gerenciais;
Prospecção, concepção e construção de fluxos e controles para melhoria dos serviços	Elaboração de documentos com processo e atividades desempenhadas pela equipe para a base de conhecimento;
	Definir e documentar estratégias para melhoria das operações de segurança ofensivas;
	Coordenar as atividades de melhoria e evolução da maturidade dos serviços;
Apoio em projetos	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Acompanhamento e revisão das políticas de segurança que envolvem as soluções e serviços sob responsabilidade da equipe de Operação Ofensivas;
	Apoio no programa de conscientização;
	Apoio na execução de exercícios de simulação (*TableTop*).

12.8. Atividades da US - 6 - Serviço de Suporte ao Gerenciamento de Projetos e Melhorias

MACROATIVIDADES	ATIVIDADES
Liderar e coordenar as atividades técnicas de suporte ao gerenciamento de projetos e melhorias	Desenvolvimento das atividades de suporte ao gerenciamento de portfólio de projetos e melhorias;
	Suporte ao gerenciamento da implantação de projetos e melhorias;
	Realizar o planejamento de atividades, definindo prazos e estratégias de priorização;
	Acompanhar e monitorar as entregas e os indicadores de qualidade do serviço;
Apoio às atividades técnicas	Apoio consultivo no planejamento e implantações de mudanças, políticas de segurança, normas, diretrizes e procedimentos;
	Auxiliar equipe técnica ou de consultoria na elaboração do documento de Requisição de Mudança (RDM);
	Negociar janela de implantação com equipe responsável no Ambiente de Operação de TI

MACROATIVIDADES	ATIVIDADES
	Abrir RDM junto à equipe responsável no Ambiente de Operação de TI;
	Acompanhar a solicitação, planejamento, implantação, teste de conformidade e encerramento de RDMs relacionadas a projetos e melhorias;
	Desenvolver e coordenar a implantação de projetos em soluções de Segurança da Informação, Prevenção a Fraude e de TI, já utilizadas pelo CONTRATANTE ou em novas soluções adquiridas/desenvolvidas internamente.
	Desenvolver e coordenar a implantação de melhorias em soluções de Segurança da Informação, Prevenção a Fraude e de TI, já utilizadas pelo CONTRATANTE ou em novas soluções adquiridas/desenvolvidas internamente.
	Elaboração de apresentações executivas de evolução dos projetos;
Suporte às atividades de gerenciamento de projetos e melhorias	Apoiar o Gerente de Projetos do CONTRATANTE na elaboração dos documentos dos projetos, tais como: • Termos de Abertura; • Declaração do Escopo; • EAP – Estrutura Analítica do Projeto; • Matriz de Responsabilidades; • Matriz de Comunicação; • Lista de riscos e plano de resposta aos riscos do projeto; • Cronogramas; • Atas de reuniões. Obs.: A documentação necessária ao gerenciamento do projeto será definida pelo CONTRATANTE na abertura do projeto.
	Apoiar o Gerente de Projetos do CONTRATANTE em atividades, tais como: • mapear, monitorar e controlar os riscos dos projetos; • elaborar e atualizar os cronogramas dos projetos; • realizar e/ou participar de reuniões de apresentação, de acompanhamento e de encerramento dos projetos; • elaborar Relatórios de Acompanhamento dos Projetos (RAP) semanalmente; • acompanhar ações realizadas durante a execução do projeto, para assegurar que os diversos elementos estejam adequadamente coordenados; • registrar lições aprendidas nos projetos; • atualizar portfólio de projetos; • oferecer suporte às atividades inerentes ao período de pós implantação de projetos; • oferecer suporte às atividades de validação de entregáveis pertencentes ao escopo do projeto.
	Apoiar o CONTRATANTE em atividades de acompanhamento e execução de melhorias em recursos de Segurança da Informação e das demais unidades de serviços do contrato;
	Apoiar o CONTRATANTE na realização das seguintes atividades referentes a aquisições de soluções de segurança da informação e das demais unidades de serviços do contrato: Elaboração de artefatos, acompanhamento das aquisições, atualização de status, encaminhamento de documentações internas.
	Manter e gerenciar toda a documentação produzida e necessária para a execução dos projetos e melhorias, mantendo no portfólio de projetos do Contratante (ambiente SharePoint).
	Possuir documentação de controle (mantendo no portfólio de projetos do Contratante - ambiente SharePoint) acerca de todos os projetos e melhorias de Segurança da Informação e das demais unidades de serviços do contrato, possuindo, em tempo real, informações tais como: Relação dos projetos e melhorias, respectivos status, estimativas e previsões de custos, controle de desembolsos, controle de prazos, responsáveis, recursos alocados, controle de

MACROATIVIDADES	ATIVIDADES
	replanejamentos, projeções, dentre outras.
	Disponibilizar e manter atualizadas, em *Dashboards* gerenciais (mantendo no portfólio de projetos do Contratante - ambiente SharePoint), todas as informações referentes ao gerenciamento de portfólio de projetos e melhorias de Segurança da Informação e das demais unidades de serviços do contrato;
	Elaborar e apresentar, semanalmente, status das ações realizadas dentro do escopo do processo em questão.
	Elaborar e apresentar, mensalmente, status das ações realizadas dentro do escopo do processo em questão.
Prospecção, concepção, construção e melhorias dos projetos e dos planos de projetos	Definição e especificação dos requisitos e escopo do projeto;
	Pesquisar e analisar cenários, tendências e melhores práticas do mercado referentes à sua área de atuação e de acordo com as necessidades do CONTRATANTE;
	Prospectar soluções tecnológicas de mercado direcionadas aos projetos de Segurança da Informação, Prevenção a Fraude e de TI.

12.9. Atividades da US - 7 - Serviço de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)

12.9.1. Perfil I - Especialista Nível I

MACROATIVIDADES	ATIVIDADES
Elaboração dos Documentos e gerenciamento da Base de Conhecimento	Criação, Edição e Manutenção de Documentos da Base de Conhecimento do Grupo de Resposta a Incidentes de Segurança e das demais unidades de serviços do contrato;
	Documentar e submeter à Base de Conhecimento, informações como solução de contorno, erro conhecido, solução definitiva, documentos de construção e teste, bem como demais instruções e procedimentos de trabalho que se julguem necessários a serem importados para a Base de Conhecimento;
	Avaliar documento de conhecimento sugerido e identificar: • se o mesmo é tecnicamente viável; • se o mesmo já existe na base; • se o mesmo pode ser um complemento de uma solução existente; • se o mesmo pode ser incluso com outros documentos propostos;
	Indicar qual a categorização do documento;
	Avaliar documento de conhecimento sugerido e identificar se o mesmo faz parte do escopo da Base de Conhecimento;
	Notificar a não validação de um documento registrado na Base de Conhecimento;
	Interagir continuamente com os proprietários dos processos correlatos;
	Garantir a integridade e atualização dos documentos, atualizando-os sempre que necessário;
	Gerar informações de auditoria na Base de Conhecimento, apontando desvios nos tempos de validação / publicação dos documentos de conhecimento, bem como no preenchimento da documentação dos mesmos, aperfeiçoando-os quando necessário.
Prospecção, concepção e construção de padrões, modelos e controles para melhoria dos	Padronização de Documentos para Base de Conhecimento, Modelo de Maturidade e Processos do Grupos de Resposta a Incidentes de Segurança e dos processos das demais unidades de serviços do contrato;
	Monitorar o progresso da geração do documento de conhecimento, desde o seu registro até a publicação, incluindo acompanhamento dos ajustes necessários;

MACROATIVIDADES	ATIVIDADES
serviços	
Apoio as atividades de gestão de conhecimento	Apoio na elaboração e execução de Campanhas de Conscientização;
	Apoio no desenvolvimento de atividades de treinamento e capacitação sobre a temática de Segurança da Informação;
	Apoio nas atividades de melhoria dos processos e modelos de maturidade.
	Apoio na execução e coleta de informações das avaliações dos modelos de maturidade e postura de segurança.

12.9.2. Perfil II - Especialista Nível II

MACROATIVIDADES	ATIVIDADES
Elaboração de campanhas de conscientização	Mapear temas e abordagens que podem ser utilizadas nas campanhas;
	Elaboração de conteúdo que será trabalhado nas Campanhas de Conscientização;
	Criação de controle de acompanhamento dos colaboradores durante a execução das campanhas;
Elaboração de treinamentos e *worshops*	Mapeamento das competências técnicas e comportamentais para as unidades de serviços do contrato;
	Desenvolvimento de atividades de treinamento e capacitação sobre a temática de Segurança da Informação e das demais unidades de serviços do contrato;
	Criação de controle de acompanhamento dos treinamentos da equipe;
	Medir a absorção do conhecimento e realizar ações para melhorar a absorção caso não seja satisfatória;
	Garantir que todos os profissionais do CONTRATADO conheçam as informações de processos necessários para execução de suas atividades com qualidade;
	Assegurar, através da transferência de conhecimento, a adaptação da atualização solicitada pelo CONTRATANTE dos produtos, processos e tecnologias utilizados;
Gerenciamento de maturidade da documentação dos processos / serviços / atividades	Padronização de Documentos para Modelo de Maturidade e Processos do Grupos de Resposta a Incidentes de Segurança e dos processos das demais unidades de serviços do contrato;
	Executar diagnóstico periódico de maturidade dos processos, fluxos e outros serviços de Segurança da Informação e das demais unidades de serviços do contrato;
	Elaborar plano de ação focado em melhorias e evolução de maturidade para os processos, fluxos e outros serviços de Segurança da Informação e das demais unidades de serviços do contrato;
	Executar avaliação dos modelos de maturidades e postura de segurança, coletando todos os dados necessários com as áreas necessária do CONTRATANTE;
	Elaboração de plano de ação focado nas melhorias dos modelos de maturidade e postura de segurança;
	Criação de controle de acompanhamento das ações dos planos de ações criados;

12.9.3. Perfil III - Especialista Nível III

MACROATIVIDADES	ATIVIDADES
Elaboração de processos e fluxos	Criação, Edição e Manutenção de Processos e fluxos do Grupo de Resposta a Incidentes de Segurança e das demais unidades de serviços do contrato;
	Desenhar, redesenhar e controlar o versionamento dos processos e fluxos de Segurança da Informação e das demais unidades de serviços do contrato;
	Manutenção dos documentos dos modelos de maturidade;
	Avaliar documento de conhecimento sugerido e identificar:

MACROATIVIDADES	ATIVIDADES
	• se o mesmo é tecnicamente viável; • se o mesmo já existe na base; • se o mesmo pode ser um complemento de uma solução existente; • se o mesmo pode ser incluso com outros documentos propostos;
	Interagir continuamente com os proprietários dos processos correlatos;
	Garantir a integridade e atualização dos documentos, atualizando-os sempre que necessário;
	Mapear e otimizar os processos de Segurança da Informação e das demais unidades de serviços do contrato, identificando gaps e propondo melhorias;
	Gerar informações de auditoria na Base de Conhecimento, apontando desvios nos tempos de validação / publicação dos documentos de conhecimento, bem como no preenchimento da documentação dos mesmos, aperfeiçoando-os quando necessário;
Prospecção, concepção e construção de padrões, modelos e controles para melhoria dos serviços	Gerenciar a adaptação de eventuais solicitações do CONTRANTE quanto a atualização de suas normas, padrões, processos, procedimentos e modelos de maturidade;
	Construir/atualizar do Catálogo de Serviços de Segurança da informação e das demais unidades de serviços do contrato;
	Padronização de Documentos do Modelo de Maturidade e Processos do Grupos de Resposta a Incidentes de Segurança e dos processos das demais unidades de serviços do contrato;
	Monitorar o progresso da geração de processos e fluxos, desde a sua criação até a conclusão, incluindo acompanhamento dos ajustes necessários.
Gerenciamento de desempenho dos processos e fluxos	Realizar avaliações periódicas do desempenho dos processos de Segurança da Informação e das demais unidades de serviços do contrato;
	Mensurar e apresentar, através de *dashboards*, os indicadores de desempenho da Segurança da Informação;
	Preparar *dashboard* com os resultados das avaliações e acompanhar a execução das ações de correções/melhorias encontradas;
Apoio as atividades de gestão de conhecimento	Elaboração de modelos de documentos para treinamentos, modelos de maturidade, avaliação de postura de segurança, relatórios e outros documentos utilizados pela equipe do contrato;
	Elaboração de conteúdo que será trabalhado nas Campanhas de Conscientização;
	Criação de controle de acompanhamento dos colaboradores durante a execução das campanhas;

12.10. Atividades da US - 8 – Serviço de Suporte ao Gerenciamento de Dados

MACROATIVIDADES	ATIVIDADES
Business Intelligence	Analisar e levantar requisitos;
	Validar dados coletados;
	Gerar relatórios, *dashboards* entre outras formas de visualizações para tomada de decisão;
Manipulação de Dados	Coletar dados de fontes primárias e secundárias;
	Consultar bancos de dados SQL para fazer análises preliminares;
	Executar e manipular grandes conjuntos de dados em bancos de dados;
Apoio as atividades de gestão de conhecimento	Criação de *dashboards* gerenciais de dados dos treinamentos, modelos de maturidade, avaliação de postura de segurança, relatórios e outros serviços utilizados pela equipe do contrato;
	Elaborar painéis de gerenciamento de dados dos treinamentos, modelos de

MACROATIVIDADES	ATIVIDADES
	maturidade, avaliação de postura de segurança, relatórios e outros serviços utilizados pela equipe do contrato;
	Criação de formulários para coletas de informações dos serviços utilizados pela equipe do contrato;
	Criação de *bots* para apoio nas dúvidas de usuários;

12.11. **Atividades da US - 9 – Serviço de Segurança da Informação e Cibernética (Operações de Segurança I)**

MACROATIVIDADES	ATIVIDADES
Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições	Verificar e acompanhar todas as requisições em relação às atividades de registro, atendimento, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Garantir o preenchimento das informações e atualizações de estado no sistema disponibilizado pelo CONTRATANTE;
	Notificar ao CONTRATANTE quaisquer anormalidades que possam causar impacto nas atividades;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento da Requisição;
	Justificar, quando necessário, o porquê da utilização de determinados status no atendimento da requisição para o demandante, de tal forma que seja possível entender claramente o motivo pelo qual a requisição passou para aquele status;
	Manter os logs das requisições devidamente atualizados quando colocadas no status de pendência, considerando a periodicidade definida pelo CONTRATANTE, registrando informações sobre contatos realizados com o usuário final da demanda ou parceiro externo visando solucionar a demanda;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Realizar as atividades solicitadas na requisição, dentre elas: • validar a realização de provas de conceito de recursos de TI; • validar soluções de Segurança e/ou TI; • realizar conferência e emissão de parecer técnico sobre a entrega de soluções de Segurança e/ou TI contratadas; • automatizar procedimentos e rotinas utilizando funcionalidades disponíveis em softwares em uso pelo CONTRATANTE; • instalação, desinstalação, manutenção, aplicação de correção, customização e parametrização, atualização de versões de componentes, alteração e adaptação de configurações, implantação de funcionalidades suportadas de software; • avaliação das necessidades de mudanças de versões / *releases* de software; • abertura, apoio e acompanhamento de chamados junto a fornecedores, conforme orientações do CONTRATANTE;
	Coletar e incluir na demanda evidência(s) do atendimento da requisição de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Documentar o atendimento realizado e, se for o caso, submeter à base de conhecimento de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Retornar a requisição à equipe de classificadores para o devido fechamento;
	Verificar se as informações da requisição estão corretamente preenchidas, conforme definições do CONTRATANTE;
	Verificar se as informações de documentação das atividades realizadas para o

MACROATIVIDADES	ATIVIDADES
	atendimento da demanda estão corretamente preenchidas, conforme definições do CONTRATANTE, tais como: procedimentos realizados para atendimento da requisição, evidências de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, documento(s) da base de conhecimento utilizado(s), requisições filhas relacionadas, dentre outras;
	Retornar para a equipe técnica as requisições que não contiverem as informações mínimas requisitadas no item acima, para que estas sejam documentadas, ampla e detalhadamente, de forma que um usuário comum consiga entender claramente o que foi realizado durante todo o atendimento da requisição, desde a sua abertura;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas ao atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc.
Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos	Configuração, manutenção, suporte e operacionalização aos equipamentos, sistemas e softwares de operações e correlacionamento de eventos e alertas de segurança, inteligência de ameaças cibernéticas e automação dos serviços de segurança;
	Realizar todas as operações de administração, gerenciamento e monitoramento das ferramentas e serviços, incluindo, mas não se limitando a: • Coleta de logs; • Criação de regras de correlação, não havendo limites mínimo ou máximo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados; • Realização de configurações; • Interação com os fabricantes das soluções; • Interação com a equipe técnica responsável pela configuração do envio de logs nos ativos monitorados; • *Backup* e *restore*; • Resolução de problemas; • Suporte; • Atualização, de acordo com as recomendações do fabricante;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade;
	Atuar de forma preventiva na detecção de falhas e solucionar ocorrências em tempo de produção de acordo com as normas e padrões determinados pelo CONTRATANTE;
	Manter os módulos das soluções e serviços atualizados, 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;
	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Monitoramento dos serviços de automação de segurança e inteligência de ameaças cibernéticas, correlação de eventos e alertas de segurança;
	Detecção, investigação, diagnóstico e solução de anomalias e padrões de comportamento;
	Detecção, investigação, diagnóstico e solução de padrões em logs e outros valores;

MACROATIVIDADES	ATIVIDADES
	Detecção, investigação, diagnóstico e solução de anomalias baseadas em tendência;
	Realizar a integração assistida dos sensores de segurança do Banco do Nordeste com a Solução Integrada de SOC, 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;
	Documentar e atualizar procedimentos de Operação e Monitoração.
Apoio em Projetos	Apoiar e prover insumos para pesquisas para automação dos serviços de inteligência e segurança da informação;
	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de SIEM e de Inteligência de Ameaças.

12.12. Atividades da US - 10 – Serviço de Segurança da Informação e Cibernética (Operações de Segurança II)

MACROATIVIDADES	ATIVIDADES
Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições	Verificar e acompanhar todas as requisições em relação às atividades de registro, atendimento, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Garantir o preenchimento das informações e atualizações de estado no sistema disponibilizado pelo CONTRATANTE;
	Notificar o CONTRATANTE quaisquer anormalidades que possam causar impacto nas atividades;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento da Requisição;
	Justificar, quando necessário, o porquê da utilização de determinados status no atendimento da requisição para o demandante, de tal forma que seja possível entender claramente o motivo pelo qual a requisição passou para aquele status;
	Manter os logs das requisições devidamente atualizados quando colocadas no status de pendência, considerando a periodicidade definida pelo CONTRATANTE, registrando informações sobre contatos realizados com o usuário final da demanda ou parceiro externo visando solucionar a demanda;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Realizar as atividades solicitadas na requisição, dentre elas: • validar a realização de provas de conceito de recursos de TI; • validar soluções de Segurança e/ou TI; • realizar conferência e emissão de parecer técnico sobre a entrega de soluções

MACROATIVIDADES	ATIVIDADES
	de Segurança e/ou TI contratadas; • automatizar procedimentos e rotinas utilizando funcionalidades disponíveis em softwares em uso pelo CONTRATANTE; • instalação, desinstalação, manutenção, aplicação de correção, customização e parametrização, atualização de versões de componentes, alteração e adaptação de configurações, implantação de funcionalidades suportadas de software; • avaliação das necessidades de mudanças de versões / releases de software; • abertura, apoio e acompanhamento de chamados junto a fornecedores, conforme orientações do CONTRATANTE.
	Coletar e incluir na demanda evidência(s) do atendimento da requisição de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Documentar o atendimento realizado e, se for o caso, submeter à base de conhecimento de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Retornar a requisição à equipe de classificadores para o devido fechamento;
	Verificar se as informações da requisição estão corretamente preenchidas, conforme definições do CONTRATANTE;
	Verificar se as informações de documentação das atividades realizadas para o atendimento da demanda estão corretamente preenchidas, conforme definições do CONTRATANTE, tais como: procedimentos realizados para atendimento da requisição, evidências de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, documento(s) da base de conhecimento utilizado(s), requisições filhas relacionadas, dentre outras;
	Retornar para a equipe técnica as requisições que não contiverem as informações mínimas requisitadas no item acima, para que estas sejam documentadas, ampla e detalhadamente, de forma que um usuário comum consiga entender claramente o que foi realizado durante todo o atendimento da requisição, desde a sua abertura;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas ao atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc.
Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos	Configuração, manutenção, suporte e operacionalização aos equipamentos, sistemas, *softwares* e serviços do O365, DLP e CASB;
	Realizar todas as operações de administração, gerenciamento e monitoramento das ferramentas e serviços, incluindo, mas não se limitando a: • Criação/manutenção de políticas; • Coleta de logs; • Realização de configurações; • Interação com os fabricantes das soluções; • *Backup* e *restore*; • Resolução de problemas; • Suporte; • Atualização, de acordo com as recomendações do fabricante;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade;
	Atuar de forma preventiva na detecção de falhas e solucionar ocorrências em tempo de produção de acordo com as normas e padrões determinados pelo CONTRATANTE;
	Manter os módulos das soluções e serviços atualizados, instalar *patches*, correções e versões ou releases mais recentes dos softwares, provisionamento dos serviços

MACROATIVIDADES	ATIVIDADES
	de configuração e implementação de facilidades de configuração para atualização ou modificação dos recursos lógicos dos módulos da solução;
	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Executar procedimentos para fazer o ajuste fino (*tunning*) das soluções sob sua responsabilidade, adequando-a ao ambiente do Banco do Nordeste e realizando as customizações de configuração necessárias;
	Realizar configuração de regras nas soluções sob sua responsabilidade, de forma proativa ou sempre que solicitada pelo Banco do Nordeste, permitindo a detecção de ameaças ao ambiente do Banco do Nordeste;
	Manter as regras atualizadas, de modo a refletir a ocorrência de novas ameaças, novas políticas de alarme e atualizações de padrões de classificação das informações;
	Monitoramento dos serviços de O365, fluxo de mensagens de e-mail e de classificação das informações;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Documentar e atualizar procedimentos de Operação e Monitoração.
Apoio em Projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de O365, DLP e CASB;
	Apoio nas campanhas de conscientizações através dos serviços do O365.

12.13. **Atividades da US - 11 – Serviço de Segurança da Informação e Cibernética (Operações de Segurança III)**

MACROATIVIDADES	ATIVIDADES
Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições	Verificar e acompanhar todas as requisições em relação às atividades de registro, atendimento, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Garantir o preenchimento das informações e atualizações de estado no sistema disponibilizado pelo CONTRATANTE;
	Notificar o CONTRATANTE quaisquer anormalidades que possam causar impacto nas atividades;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento da Requisição;
	Justificar, quando necessário, o porquê da utilização de determinados status no atendimento da requisição para o demandante, de tal forma que seja possível entender claramente o motivo pelo qual a requisição passou para aquele status;
	Manter os logs das requisições devidamente atualizados quando colocadas no status de pendência, considerando a periodicidade definida pelo CONTRATANTE, registrando informações sobre contatos realizados com o usuário final da demanda ou parceiro externo visando solucionar a demanda;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Realizar as atividades solicitadas na requisição, dentre elas: • validar a realização de provas de conceito de recursos de TI; • validar soluções de Segurança e/ou TI;

MACROATIVIDADES	ATIVIDADES
	• realizar conferência e emissão de parecer técnico sobre a entrega de soluções de Segurança e/ou TI contratadas; • automatizar procedimentos e rotinas utilizando funcionalidades disponíveis em softwares em uso pelo CONTRATANTE; • instalação, desinstalação, manutenção, aplicação de correção, customização e parametrização, atualização de versões de componentes, alteração e adaptação de configurações, implantação de funcionalidades suportadas de software; • avaliação das necessidades de mudanças de versões / releases de software; • abertura, apoio e acompanhamento de chamados junto a fornecedores, conforme orientações do CONTRATANTE.
	Coletar e incluir na demanda evidência(s) do atendimento da requisição de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Documentar o atendimento realizado e, se for o caso, submeter à base de conhecimento de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Retornar a requisição à equipe de classificadores para o devido fechamento;
	Verificar se as informações da requisição estão corretamente preenchidas, conforme definições do CONTRATANTE;
	Verificar se as informações de documentação das atividades realizadas para o atendimento da demanda estão corretamente preenchidas, conforme definições do CONTRATANTE, tais como: procedimentos realizados para atendimento da requisição, evidências de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, documento(s) da base de conhecimento utilizado(s), requisições filhas relacionadas, dentre outras;
	Retornar para a equipe técnica as requisições que não contiverem as informações mínimas requisitadas no item acima, para que estas sejam documentadas, ampla e detalhadamente, de forma que um usuário comum consiga entender claramente o que foi realizado durante todo o atendimento da requisição, desde a sua abertura;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas ao atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc.
Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos	Configuração, manutenção e suporte aos equipamentos, sistemas e softwares de Certificados Digitais, HSM e Gestão de Identidades e Acesso;
	Realizar todas as operações de administração, gerenciamento e monitoramento das ferramentas e serviços, incluindo, mas não se limitando a: • Criação/manutenção de políticas; • Coleta de logs; • Realização de configurações; • Interação com os fabricantes das soluções; • *Backup* e *restore*; • Resolução de problemas; • Suporte; • Atualização, de acordo com as recomendações do fabricante;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade;
	Atuar de forma preventiva na detecção de falhas e solucionar ocorrências em tempo de produção de acordo com as normas e padrões determinados pelo CONTRATANTE;

MACROATIVIDADES	ATIVIDADES
	Manter os módulos das soluções e serviços atualizados, 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;
	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Monitoramento dos serviços de Certificados Digitais, HSM e Gestão de Identidades e Acesso;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Apoio a aquisição de certificados digitais externo, realizando todo o levantamento técnico com base nos requisitos do sistema ou serviço;
	Emissão e Revogação de Certificados Digitais interno;
	Suporte a equipe responsável pela instalação dos certificados;
	Documentar e atualizar procedimentos de Operação e Monitoração.
Apoio em Projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de HSM, GIA e Certificados Digitais.

12.14. **Atividades da US - 12 – Serviço de Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)**

MACROATIVIDADES	ATIVIDADES
Classificação de Incidentes, Problemas e Requisições	Identificar a demanda (Incidente, Problema ou Requisição) e realizar a devida classificação, devendo, caso seja necessário, converter o Incidente em Requisição de Serviço ou em Requisição de Mudança e vice-versa, dentre outras conversões possíveis;
	Verificar e inserir, em sistema disponibilizado pelo CONTRATANTE, informações referentes ao correto grupo de atendimento, categoria, prioridade, impacto, urgência, item de configuração, status do item de configuração, dentre outras informações relacionadas à macroatividade de classificação de demanda e de requisições;
	Encaminhar a demanda para a equipe técnica, após a completa e correta classificação desta;
	Comunicar ao demandante, caso necessário, o resultado da categorização, o prazo estimado de atendimento da requisição de serviço, os contatos para informações adicionais, dentre outros.
Triagem dos Alertas de Segurança	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;
	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;
	Os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado;
	Avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no *baseline*;

MACROATIVIDADES	ATIVIDADES
Monitoramento, Acompanhamento e Comunicação de Incidentes e Alertas de Segurança	Verificar e acompanhar todos os Incidentes ou Problemas em relação às atividades de registro, atendimento, investigação, diagnóstico, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Notificar o CONTRATANTE quaisquer anormalidades que possam causar impacto nos serviços;
	Reportar ao CONTRATANTE, a cada hora, o status da evolução do atendimento a incidentes ou a problemas considerados mais críticos conforme definição do CONTRATANTE;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento do Incidente ou do Problema;
	Preparar relatórios gerenciais sobre os incidentes resolvidos de acordo com a demanda do CONTRATANTE;
	Vincular os Incidentes ou problemas relacionados, isto é, incidente pai com Incidente(s) filho(s), etc.
Investigação, diagnóstico, resolução e encerramento de Requisições de Serviços e Incidentes de Segurança.	Realizar o diagnóstico inicial dos incidentes e problemas previamente classificados e encaminhados para a equipe técnica;
	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;
	Identificar possíveis soluções definitivas ou de contorno para o Incidente ou problema;
	Providenciar subsídios para os casos de abertura e acompanhamento de chamados junto a fornecedores;
	Aplicar a solução para o incidente ou problema visando restaurar o mais rápido possível o serviço/componente afetado;
	Registrar todas as requisições de mudança necessárias para a implantação de soluções de contorno a incidentes ou problemas;
	Realizar os devidos testes para confirmar que o incidente ou problema foi solucionado;
	Documentar a solução adotada para o incidente ou problema e submeter à base de conhecimento;
	Verificar se as informações de documentação das atividades realizadas para o atendimento da demanda, desde a abertura desta, estão corretamente preenchidas, tais como: procedimentos realizados para atendimento, evidências (*printscreen*, logs etc.) de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, causa da

MACROATIVIDADES	ATIVIDADES
	ocorrência do Incidente, solução de contorno aplicada, documento(s) da base de conhecimento utilizado(s), requisições ou incidentes filhos relacionados, dentre outras;
	As evidências de comprovação de procedimentos realizados deverão conter as informações de data e hora, bem como a descrição da evidência em si;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas à solução do incidente, problema ou atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc;
	Realizar o diagnóstico inicial dos incidentes e problemas previamente classificados e encaminhados para a equipe técnica;
	Documentar e atualizar procedimentos de Operação e Monitoração.

12.15. Atividades da US - 13 – Serviço de Segurança da Informação e Cibernética (Operações Defensivas)

12.15.1. Perfil I – Especialista Nível I

MACROATIVIDADES	ATIVIDADES
Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições	Verificar e acompanhar todas as requisições em relação às atividades de registro, atendimento, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Garantir o preenchimento das informações e atualizações de estado no sistema disponibilizado pelo CONTRATANTE;
	Notificar o CONTRATANTE quaisquer anormalidades que possam causar impacto nas atividades;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento da Requisição;
	Justificar, quando necessário, o porquê da utilização de determinados status no atendimento da requisição para o demandante, de tal forma que seja possível entender claramente o motivo pelo qual a requisição passou para aquele status;
	Manter os logs das requisições devidamente atualizados quando colocadas no status de pendência, considerando a periodicidade definida pelo CONTRATANTE, registrando informações sobre contatos realizados com o usuário final da demanda ou parceiro externo visando solucionar a demanda;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Realizar as atividades solicitadas na requisição, dentre elas: • validar a realização de provas de conceito de recursos de TI; • validar soluções de Segurança e/ou TI; • realizar conferência e emissão de parecer técnico sobre a entrega de soluções de Segurança e/ou TI contratadas; • automatizar procedimentos e rotinas utilizando funcionalidades disponíveis em softwares em uso pelo CONTRATANTE; • instalação, desinstalação, manutenção, aplicação de correção, customização e parametrização, atualização de versões de componentes, alteração e adaptação de configurações, implantação de funcionalidades suportadas de software; • avaliação das necessidades de mudanças de versões / releases de software; • abertura, apoio e acompanhamento de chamados junto a fornecedores, conforme orientações do CONTRATANTE;

MACROATIVIDADES	ATIVIDADES
	Coletar e incluir na demanda evidência(s) do atendimento da requisição de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Documentar o atendimento realizado e, se for o caso, submeter à base de conhecimento de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Retornar a requisição à equipe de classificadores para o devido fechamento;
	Verificar se as informações da requisição estão corretamente preenchidas, conforme definições do CONTRATANTE;
	Verificar se as informações de documentação das atividades realizadas para o atendimento da demanda estão corretamente preenchidas, conforme definições do CONTRATANTE, tais como: procedimentos realizados para atendimento da requisição, evidências de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, documento(s) da base de conhecimento utilizado(s), requisições filhas relacionadas, dentre outras;
	Retornar para a equipe técnica as requisições que não contiverem as informações mínimas requisitadas no item acima, para que estas sejam documentadas, ampla e detalhadamente, de forma que um usuário comum consiga entender claramente o que foi realizado durante todo o atendimento da requisição, desde a sua abertura;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas ao atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc.
Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos	Configuração, manutenção e suporte aos equipamentos, sistemas e softwares de firewall, SSE, EDR, WAF, internet, computação em nuvem e GAV;
	Realizar todas as operações de administração, gerenciamento e monitoramento das ferramentas e serviços, incluindo, mas não se limitando a: • Criação/manutenção de políticas; • Coleta de logs; • Realização de configurações; • Interação com os fabricantes das soluções; • *Backup* e *restore*; • Resolução de problemas; • Suporte; • Atualização, de acordo com as recomendações do fabricante;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade;
	Atuar de forma preventiva na detecção de falhas e solucionar ocorrências em tempo de produção de acordo com as normas e padrões determinados pelo CONTRATANTE;
	Manter os módulos das soluções e serviços atualizados, 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;
	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Monitoramento dos serviços de rede, conectividade, firewall, SSE (*Security Service Edge*), EDR (*Endpoint Detection and Response*), WAF (*Web Application Firewall*), computação em nuvem e Gestão de Vulnerabilidades;

MACROATIVIDADES	ATIVIDADES
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Gerenciamento das vulnerabilidades do ambiente;
	Documentar e atualizar procedimentos de Operação e Monitoração.
Apoio em Projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de firewall, SSE (*Security Service Edge*), EDR (*Endpoint Detection and Response*), WAF (*Web Application Firewall*), computação em nuvem e Gestão de Vulnerabilidades.

12.15.2. Perfil II – Especialista Nível II

MACROATIVIDADES	ATIVIDADES
Monitoramento, Atendimento, Acompanhamento, Encerramento e Comunicação de Requisições	Verificar e acompanhar todas as requisições em relação às atividades de registro, atendimento, escalonamento, cumprimento de prazos, qualidade das informações, dentre outros;
	Garantir o preenchimento das informações e atualizações de estado no sistema disponibilizado pelo CONTRATANTE;
	Notificar o CONTRATANTE quaisquer anormalidades que possam causar impacto nas atividades;
	Comunicar-se, quando necessário, com o usuário final da demanda, parceiro externo ou com o CONTRATANTE, de forma a obter informações decisórias, operacionais ou gerenciais necessárias e inerentes à busca da solução e/ou atendimento da Requisição;
	Justificar, quando necessário, o porquê da utilização de determinados status no atendimento da requisição para o demandante, de tal forma que seja possível entender claramente o motivo pelo qual a requisição passou para aquele status;
	Manter os logs das requisições devidamente atualizados quando colocadas no status de pendência, considerando a periodicidade definida pelo CONTRATANTE, registrando informações sobre contatos realizados com o usuário final da demanda ou parceiro externo visando solucionar a demanda;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Realizar as atividades solicitadas na requisição, dentre elas: • validar a realização de provas de conceito de recursos de TI; • validar soluções de Segurança e/ou TI; • realizar conferência e emissão de parecer técnico sobre a entrega de soluções de Segurança e/ou TI contratadas; • automatizar procedimentos e rotinas utilizando funcionalidades disponíveis em softwares em uso pelo CONTRATANTE; • instalação, desinstalação, manutenção, aplicação de correção, customização e parametrização, atualização de versões de componentes, alteração e adaptação de configurações, implantação de funcionalidades suportadas de software; • avaliação das necessidades de mudanças de versões / releases de software; • abertura, apoio e acompanhamento de chamados junto a fornecedores, conforme orientações do CONTRATANTE;
	Coletar e incluir na demanda evidência(s) do atendimento da requisição de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Documentar o atendimento realizado e, se for o caso, submeter à base de conhecimento de acordo com os padrões estabelecidos pelo CONTRATANTE;
	Retornar a requisição à equipe de classificadores para o devido fechamento;
	Verificar se as informações da requisição estão corretamente preenchidas, conforme definições do CONTRATANTE;

MACROATIVIDADES	ATIVIDADES
	Verificar se as informações de documentação das atividades realizadas para o atendimento da demanda estão corretamente preenchidas, conforme definições do CONTRATANTE, tais como: procedimentos realizados para atendimento da requisição, evidências de comprovação dos procedimentos realizados, itens de configuração afetados na aplicação dos procedimentos de atendimento, documento(s) da base de conhecimento utilizado(s), requisições filhas relacionadas, dentre outras;
	Retornar para a equipe técnica as requisições que não contiverem as informações mínimas requisitadas no item acima, para que estas sejam documentadas, ampla e detalhadamente, de forma que um usuário comum consiga entender claramente o que foi realizado durante todo o atendimento da requisição, desde a sua abertura;
	Comunicar-se, quando necessário, com o usuário final da demanda de forma a tratar questões relativas ao atendimento da requisição, obtendo autorização para encerramento da demanda, retorno da demanda para a equipe que a atendeu, etc;
Configuração, manutenção, suporte e Operacionalização de Serviços e Recursos	Configuração, manutenção e suporte aos equipamentos, sistemas e softwares de firewall, SSE, EDR, WAF, internet, computação em nuvem e GAV;
	Realizar todas as operações de administração, gerenciamento e monitoramento das ferramentas e serviços, incluindo, mas não se limitando a: • Criação/manutenção de políticas; • Coleta de logs; • Realização de configurações; • Interação com os fabricantes das soluções; • *Backup* e *restore*; • Resolução de problemas; • Suporte; • Atualização, de acordo com as recomendações do fabricante;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade;
	Atuar de forma preventiva na detecção de falhas e solucionar ocorrências em tempo de produção de acordo com as normas e padrões determinados pelo CONTRATANTE;
	Manter os módulos das soluções e serviços atualizados, 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;
	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Monitoramento dos serviços de rede, conectividade, firewall, SSE (*Security Service Edge*), EDR (*Endpoint Detection and Response*), WAF (*Web Application Firewall*), computação em nuvem e Gestão de Vulnerabilidades;
	Investigação, diagnóstico e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Gerenciamento das vulnerabilidades do ambiente;
	Documentar e atualizar procedimentos de Operação e Monitoração.
Suporte e melhoria dos serviços	Analisar e otimizar as regras configuradas;
	Analise de requisitos técnicos para melhoria e refinamentos de regras;
	Participações de reuniões técnicas com a equipe de Operações;

MACROATIVIDADES	ATIVIDADES
Apoio em Projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de firewall, SSE (*Security Service Edge*), EDR (*Endpoint Detection and Response*), WAF (*Web Application Firewall*), computação em nuvem e Gestão de Vulnerabilidades;
	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Apoio em elaboração de parecer técnico;

12.16. **Atividades da US - 14 – Serviço de Segurança da Informação e Cibernética (Operações Ofensivas)**

12.16.1. Perfil I – Especialista Nível I

MACROATIVIDADES	ATIVIDADES
Análise de vulnerabilidades em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas;	Realizar análise de vulnerabilidade baseada em metodologia oficial, com no mínimo as seguintes fases: • Coleta de Informações; • Identificação de vulnerabilidade; • Verificação de vulnerabilidade; • Exploração de Vulnerabilidade; • Documentação;
	Realizar homologação de novos sistemas para uso seguro no Banco do Nordeste;
	Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Testes de intrusão em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas	Realizar análise de vulnerabilidade baseada em metodologia oficial, com no mínimo as seguintes fases: • Coleta de Informações; • Identificação de vulnerabilidade; • Verificação de vulnerabilidade; • Exploração de Vulnerabilidade; • Documentação;
	Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Exercícios *Red Team* em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas;	Realizar simulações conforme o plano de exercícios de *red team*;
	Utilizar táticas, técnicas e procedimentos (TTPs) sofisticados e que estejam no escopo aprovados pelo Banco do Nordeste;
	Identificar as possíveis falhas e vulnerabilidades que possam ser exploradas em um ataque real;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Monitoramento, Acompanhamento e Comunicação de Incidentes e Alertas de Segurança	Investigação, diagnósticos e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
Apoio em Projetos	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de Teste de Segurança (Análise de vulnerabilidade, Teste de Intrusão e Red Team).

12.16.2. Perfil II – Especialista Nível II

MACROATIVIDADES	ATIVIDADES
Análise de vulnerabilidades em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas;	Realizar analise de vulnerabilidade baseada em metodologia oficial, com no mínimo as seguintes fases: • Coleta de Informações; • Identificação de vulnerabilidade; • Verificação de vulnerabilidade; • Exploração de Vulnerabilidade; • Documentação;
	Realizar homologação de novos sistemas para uso seguro no Banco do Nordeste;
	Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Testes de intrusão em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas	Realizar análise de vulnerabilidade baseada em metodologia oficial, com no mínimo as seguintes fases: • Coleta de Informações; • Identificação de vulnerabilidade; • Verificação de vulnerabilidade; • Exploração de Vulnerabilidade; • Documentação;
	Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Exercícios *Red Team* em sistemas operacionais, equipamentos e dispositivos de rede, softwares e sistemas;	Apoio na elaboração de plano de exercícios de *Red Team*;
	Realizar simulações conforme o plano de exercícios de *red team*;
	Utilizar táticas, técnicas e procedimentos (TTPs) sofisticados e que estejam no escopo aprovados pelo Banco do Nordeste;
	Identificar as possíveis falhas e vulnerabilidades que possam ser exploradas em um ataque real;
	Sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;
Suporte e melhoria dos serviços	Investigação, diagnósticos e resolução de Requisições de Serviço, Incidentes de Segurança e Alertas de Segurança;
	Simulação de incidentes para identificação e apoio nos refinamentos de regras;
	Apoio em definição e simulações de cenários para novos casos de uso;
	Analisar e otimizar execução das análises de vulnerabilidades e testes de intrusão;
	Participações de reuniões técnicas com a equipe de TI;
Apoio em Projetos	Apoio nas definições de padrões e procedimento para desenvolvimento seguro;
	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Acompanhamento e revisão das políticas de segurança que envolve as soluções e serviços de Teste de Segurança (Análise de vulnerabilidade, Teste de Intrusão e *Red Team*).

12.17. **Atividades da US - 15 – Serviço de Consultoria**

12.17.1. Perfil I – Consultor de Segurança Corporativa

MACROATIVIDADES	ATIVIDADES
Suporte às atividades de	Apoiar na prospecção de Novas Tecnologias e novos Conhecimentos;
	Estudo de mercado para novas aquisições;

prospecção de Novas Tecnologias de serviços de Segurança da Informação	Estudo de mercado para melhoria de processos e serviços;
	Participação de reuniões técnicas com fornecedores;
	Realização de Prova de conceito (POC) de tecnologias;
	Elaboração de documentos técnicos para novas aquisições de serviços e soluções;
Apoio no suporte e melhorias das ferramentas e serviços de segurança da informação utilizadas no Banco do Nordeste	Apoio consultivo para instalar, configurar e atualizar as ferramentas de segurança utilizadas no Banco do Nordeste;
	Apoio consultivo nas mudanças e melhorias na arquitetura de rede do Ambiente do Banco do Nordeste;
Estudos de Viabilidade e Análise comparativas	Apoiar na definição e implementação de mecanismos futuros de monitoramento de segurança;
	Elaborar pareceres técnicos referente a segurança corporativa;
Análise de Conformidade à Leis, Regulamentações e Normas	Apoiar nas atividades de conformidade às Leis, Regulamentações e Normas;
	Apoiar no processo de implantação de controles de segurança, em conformidade com Normas, Leis e Regulamentações;
	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;
	Realizar levantamentos estatísticos para acompanhamento da conformidade dos recursos computacionais com as recomendações da política de Segurança Corporativa estabelecidas pelo Banco do Nordeste;
Apoio na definição de Políticas, Procedimentos e Diretrizes	Elaboração de proposta de conteúdo para definir e revisão de políticas de segurança da informação;
	Analisar, propor e implementar políticas de segurança de Banco de dados, Mainframe, Linux, Nuvem, Privacidade, Fraude, Criptografia, Vazamento de dados etc.;
Elaboração de documentos com as atividades desempenhadas para a base de conhecimento	Elaborar e manter documentação das atividades desempenhadas;
Levantamento de melhorias dos processos e modelos de maturidade	Apoio na elaboração e definição de novos fluxos, processos e procedimentos para o grupo de resposta a incidentes;
	Implantação de modelos de maturidades de serviços, processos e soluções de segurança;
	Orientar sobre a aplicabilidade e utilização de frameworks de segurança, exemplo: indicados pelo NIST, FIRST, Mitre, *Cyber Kill Chain*, ATT&CK, dentre outros;
	Apoio no desenvolvimento de medição de risco de soluções, serviços e processos;
Apoio consultivo à equipe técnica especialista	Apoiar na análise dos relatórios de detecção e prevenção de ataques;
	Apoiar na intervenção em caso de invasão dos sistemas e serviços do Banco do Nordeste;
	Suporte consultivo em momentos de crises cibernéticas para executivos e técnicos;
	Recomendar ações, revisar e acompanhar o progresso de planos de ação preventivos e corretivos sob contexto de Segurança;
	Apoiar nas definições, procedimentos, processos e configurações as ferramentas

	de segurança utilizadas no Banco do Nordeste;
Atividades relacionadas à análise Forense	Coleta/extração de evidências digitais;
	Forense em ambiente Windows/linux, Mobile(IOS e Android) e Redes;
	Realização de análise de *Malwares*;
	Elaboração de laudos, relatórios e pareceres.
Apoio na elaboração de Campanhas de Conscientização	Apoio na definição de temas e atividades para serem realizadas durante as campanhas;
	Apoio na revisão de conteúdo que será disseminado na campanha;
Apoio no desenvolvimento de atividades de treinamento e capacitação sobre a temática de Segurança cibernética	Apoio na definição de temas e atividades para serem realizadas durante os treinamentos;
	Apoio na revisão de conteúdo para treinamento;

12.17.2. Perfil II – Consultor DEVSECOPS

MACROATIVIDADES	ATIVIDADES
Desenvolver e suportar as atividades de *Security Development Lifecycle*	Implementar ou manter *framework* que defina as tarefas e ações de segurança realizadas em todo o processo de desenvolvimento;
	Suportar uma boa transição de DevOps para DevSecOps;
	Definição de indicadores (KPI) para as tarefas e ações de segurança realizadas em todo o processo de desenvolvimento, bem como um limite de risco que determina a progressão do código do aplicativo;
	Orientar a utilização de ferramentas e plataformas de segurança confiáveis e atualizadas;
	Orientar práticas de segurança como autenticação, autorização e criptografia ajudam a proteger os aplicativos em tempo de desenvolvimento;
	Orientar práticas internas como modelagem de ameaças, *design* defensivo e codificação segura;
	Apoiar a manutenção de inventário de contas, ferramentas e dispositivos;
	Realizar avaliação de segurança regulares em todo o ciclo de vida do *software*;
	Observar, entender e propor melhorias no processo de desenvolvimento de *software* para incluir as disciplinas e funcionalidades de segurança por padrão
Apoiar nos testes de software para validar as especificações de segurança e/ou vulnerabilidades	Recomendar ferramentas para execução dos testes ou exercícios de simulação de ataque;
	Avaliar as causas principais das vulnerabilidades e recomendar as melhores formas de correções;
	Acompanhar planos de ações de correções de vulnerabilidades;
Apoiar na difusão da cultura de Segurança da Informação no desenvolvimento Ágil, promovendo a cultura de DevSecOps	Recomendar e orientar a execução de boas práticas para o ciclo de vida seguro de desenvolvimento;
	Identificar colaboradores que se tornarão pessoas essenciais para todos os assuntos ligados à cibersegurança, esses colaboradores poderão apoiar e encorajar a mudança de mentalidade dos demais desenvolvedores;
	Atualizar a equipe de desenvolvimento sobre as tendências do mercado;
Estudos de Viabilidade e Análise comparativas	Apoiar na definição e implementação de mecanismos futuros de monitoramento de segurança;
	Elaborar pareceres em segurança da informação;

Análise de Conformidade à Leis, Regulamentações e Normas	Apoiar nas atividades de conformidade às Leis, Regulamentações e Normas;
	Apoiar no processo de implantação de controles de segurança, em conformidade com Normas, Leis e Regulamentações;
	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;
	Realizar levantamentos estatísticos para acompanhamento da conformidade dos recursos computacionais com as recomendações das políticas de Segurança da Informação estabelecidas pelo Banco do Nordeste;
Apoio na definição de Políticas, Procedimentos e Diretrizes	Elaboração de proposta de conteúdo para definir e revisão de políticas de segurança da informação;
	Analisar, propor e implementar políticas de segurança de Banco de dados, Mainframe, Linux, Nuvem, Privacidade, Criptografia, Vazamento de dados e etc;
Elaboração de documentos com as atividades desempenhadas para a base de conhecimento	Elaborar e manter documentação das atividades desempenhadas;
Apoio consultivo à equipe técnica especialista	Apoiar na análise dos relatórios de vulnerabilidades;
	Apoiar na intervenção em caso de invasão dos sistemas e serviços do Banco do Nordeste;
	Suporte consultivo em momentos de crises cibernéticas para executivos e técnicos;
	Recomendar ações, revisar e acompanhar o progresso de planos de ação preventivos e corretivos sob contexto de Segurança;
	Apoiar nas definições, procedimentos, processos e configurações as ferramentas de segurança utilizadas no Banco do Nordeste;
Apoio na elaboração de Campanhas de Conscientização	Apoio na definição de temas e atividades para serem realizadas durante as campanhas;
	Apoio na revisão de conteúdo que será disseminado na campanha;
Apoio no desenvolvimento de atividades de treinamento e capacitação sobre a temática de Desenvolvimento Seguro	Apoio na definição de temas e atividades para serem realizadas durante os treinamentos;
	Apoio na revisão de conteúdo para treinamento;

12.18. **Atividades da US - 16 – Serviço de Operações de Combate e Prevenção a Fraude**

12.18.1. Perfil I – Especialista Nível I

MACROATIVIDADES	ATIVIDADES
Monitoramento, triagem e acompanhamento de eventos	Verificar e acompanhar todos os eventos reportados por sistemas e serviços;
	Verificar e acompanhar todos os eventos reportados por agências;
	Verificação de eventos, validados por clientes, que apresentam comportamentos suspeitos;
	Notificar eventos suspeitos;
	Acompanhamento de ocorrências que foram categorizadas como suspeitas durante as análises;

12.18.2. Perfil II – Especialista Nível II

MACROATIVIDADES	ATIVIDADES
Análise e investigação de eventos	Análise detalhada em sistemas e bases internas;
	Análise detalha em fontes externas;
	Análise documental;
	Análise de contestação de transações;
	Análise de transações reportadas por outras instituições financeiras;
	Análise comportamental de clientes;
	Análise comportamental de dispositivos.
Operacionalização de sistemas, serviços e recurso tecnológicos utilizados na prevenção e combate a fraudes	Cadastro de ocorrências;
	Bloqueio/desbloqueio de dispositivos;
	Bloqueio/desbloqueio de identificador de transações;
	Inclusão de métricas de monitoramento nos sistemas, serviços e rotinas;
	Solicitação de remoção de perfis falsos em mídias sociais;
	Solicitação de *takedown* de página falsas;
Configuração, manutenção e suporte de sistemas, serviços e recurso tecnológicos utilizados na prevenção e combate a fraudes	Monitorar, analisar e controlar o desempenho de cada componente das soluções e serviços sob sua responsabilidade, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução;
	Executar procedimentos para resolução de problemas relacionadas à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos serviços ou soluções sob sua responsabilidade.
	Realizar configuração de regras nas soluções sob sua responsabilidade, de forma proativa ou sempre que solicitada pelo Banco do Nordeste, permitindo a detecção de comportamentos suspeitos ou ameaças no ambiente do Banco do Nordeste;
	Manter as regras atualizadas, de modo a refletir a ocorrência de novas ameaças, novas políticas de alarme e atualizações de padrões;
Apoio técnico	Documentar e atualizar ocorrências.
	Elaborar e manter documentação das atividades da Operação e Monitoração.

12.18.3. Perfil III – Especialista Nível III

MACROATIVIDADES	ATIVIDADES
Análise e investigação de eventos	Análise detalhada em sistemas e bases internas;
	Análise detalha em fontes externas;
	Análise documental;
	Análise de contestação de transações;
	Análise de transações reportadas por outras instituições financeiras;
	Análise comportamental de clientes;
	Análise comportamental de dispositivos.
Suporte e melhoria dos serviços	Implantação e configurações de novos serviços ou soluções tecnológicas;
	Analisar e otimizar as regras configuradas;
	Análise de requisitos técnicos para melhoria e refinamentos de regras;
	Avaliação técnica para melhoria e refinamentos scripts/rotinas;
	Participações de reuniões técnicas;
	Apoio na elaboração e definição de novos fluxos, processos e procedimentos da equipe de prevenção a fraude;
Apoio em projetos	Apoio em revisão das políticas de segurança;
	Apoio em elaboração de parecer técnico;

	Apoio durante realização de Prova de conceito (POC) de tecnologias;
	Apoiar na definição e implementação de mecanismos futuros de monitoramento;

12.19. **Atividades da US - 17 – Serviço de Operações de Combate e Prevenção à Lavagem de Dinheiro**

12.19.1. Perfil I – Especialista Nível I

MACROATIVIDADES	ATIVIDADES
Business Intelligence	Analisar e levantar requisitos;
	Validar dados coletados;
	Gerar relatórios, *dashboards* entre outras formas de visualizações para tomada de decisão;
Programação para análise de dados	Criar aplicações de análise de dados para embasar tomadas de decisão;
	Construir modelos preditivos;
	Desenvolver varreduras de monitoramento para identificação de situações atípicas de PLD/FT;
	Avaliação técnica para melhoria e refinamentos scripts/rotinas;
	Desenvolver programas utilizando infraestrutura SAS ou Python para gerenciar e manipular grandes volumes de dados;
Suporte às atividades de Análise de dados	Elaborar e manter documentação das atividades desempenhadas;
	Propor melhorias no processo de Análise de dados;

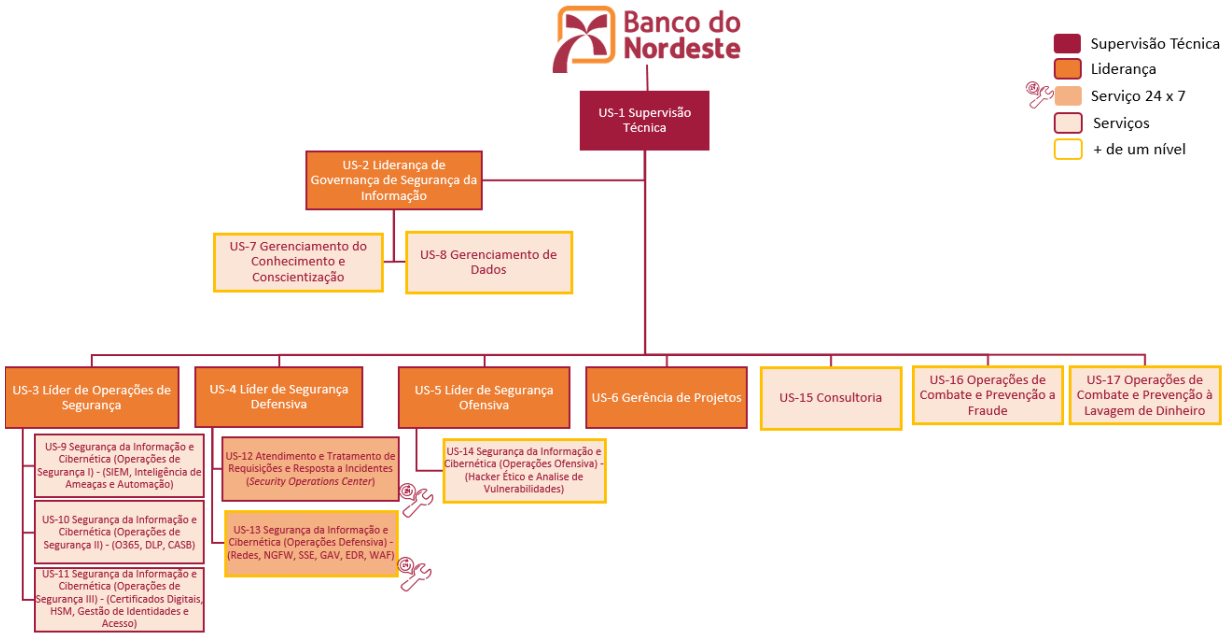
12.19.2. Perfil II – Especialista Nível II

MACROATIVIDADES	ATIVIDADES
Manipulação de Dados	Coletar dados de fontes primárias e secundárias;
	Consultar bancos de dados SQL para fazer análises preliminares;
	Conferência das cargas de dados nas bases de PLD/FT
	Gerenciar, supervisionar o armazenamento e distribuição de dados;
	Escrever e codificar programas para automatizar os processos de coleta de dados;
Business Intelligence	Gerar relatórios, *dashboards* entre outras formas de visualizações para tomada de decisão;
	Executar e manipular grandes conjuntos de dados em bancos de dados;
Suporte às atividades de Análise de dados	Elaborar e manter documentação das atividades desempenhadas;
	Propor melhorias no processo de Análise de dados;

13. CORRELAÇÃO ENTRE PROCESSOS/SERVIÇOS E PAPEIS

13.1. Para a execução dos serviços, deve-se observar a correlação entre processos/serviços e papéis conforme tabela constante do ANEXO VII;

13.2. A divisão de esferas de competência proposta está estabelecida a seguir:



13.3. Ressaltando que tais divisões de competências são propostas, cabendo à CONTRATADA definir internamente, com seus recursos, questões de hierarquização e cadeia de comando a fim de que as demandas sejam tratadas pelos profissionais competentes para atendê-las, bem como que não ocorram conflitos de competência em relação ao escopo de atuação destes profissionais.

13.4. A lista de atividades referente a cada item, bem como os requisitos obrigatórios dos perfis, poderá ser atualizado durante a vigência do Contrato em virtude de mudanças nos processos da CONTRATANTE, aquisição de novas tecnologias, mudança de paradigmas do mercado, mediante comunicação prévia à CONTRATADA.

13.5. O prazo para adequação às novas atividades, bem como para eventual readequação dos perfis, é de 90 dias.

13.6. O quantitativo de profissionais a serem diretamente envolvidos para prestação de serviços deverá ser dimensionado pela CONTRATADA de forma a garantir o atendimento das demandas de acordo com os níveis mínimos de serviço exigidos.

13.7. Cabe à CONTRATADA manter os profissionais designados para execução dos serviços plenamente capacitados e atualizados.

13.8. Sempre que for implantada uma nova tecnologia, ferramenta, ambiente ou paradigma tecnológico no ambiente de TI da CONTRATANTE, a CONTRATADA terá um prazo de 90 dias a partir da comunicação oficial da CONTRATANTE para obter as habilidades técnicas necessárias para devida prestação dos serviços na tecnologia.

13.9. Caso, sob solicitação justificada da CONTRATADA, tal nova tecnologia seja de complexidade cuja curva de aprendizagem exija tempo superior ao prazo colocado no item anterior, a CONTRATANTE pode conceder prorrogação de tal prazo por até mais 90 dias.

14. ENTREGAS PREVISTAS / FORMA DE PRESTAÇÃO DOS SERVIÇOS

14.1. Este item apresenta os produtos e/ou ações que deverão ser gerados pelo CONTRATADO necessários à execução continuada, eficiente e eficaz dos serviços que integram com as respectivas macroatividades;

14.2. Este item não contempla todas as atividades que devem ser executadas pelo CONTRATADO, bem como não detalha os passos que deverão ser dados para obtenção dos produtos de cada atividade;

14.3. As atividades para as quais as condições de atendimento/aceitação não foram definidas no momento da contratação requerem negociação de prazo e condições no momento de sua solicitação e terão estas informações especificadas na própria demanda. Por esta razão não estão contempladas neste documento;

14.4. As atividades que são executadas continuamente ou de forma rotineira pelo CONTRATADO sem a necessidade de demanda específica devem ser executadas conforme o padrão estabelecido para a sua execução e, via de regra, não estão contempladas neste documento;

14.5. A condição de aceitação para estas atividades é, além do prazo, da completude e correção do resultado esperado de cada uma, a conformidade ao padrão estabelecido para a execução;

14.6. Os relatórios especificados neste item deverão ser gerados a partir da base de dados da ferramenta de registro de demandas utilizada pelo CONTRATANTE[2], e disponibilizados em formato definido pelo CONTRATANTE, devendo ser armazenados em local designado por este;

14.7. Após a assinatura do contrato e reunião inicial entre a CONTRATANTE e CONTRATADA, **será formalizada uma Ordem de Serviço**, autorizando o início da prestação do serviço;

14.8. As entregas mensais serão apuradas considerando o período do primeiro ao último dia do mês de prestação de serviços;

14.9. Entregas:

14.9.1. Entregas do Serviço de Supervisão Técnica:

ENTREGAS	PRAZO MÁXIMO DE ENTREGA
Relatório Mensal de Nível de Serviço contendo nome do indicador, o nível alcançado, o desconto previsto no valor mensal, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual	Até o 5º (quinto) dia útil do mês subsequente ao do período do relatório
Relatório semanal de Escala de Especialistas (Equipe 24x7), mencionando quais profissionais estão preenchendo as especialidades prevista em cada dia e horário.	Até as 11h00min de todas as sextas-feiras

[2] *CA Service Desk Manager* ou outra ferramenta que venha a substitui-la

Reunião de Status Gerencial	Até o 15º (décimo quinto) dia do mês subsequente ao mês de referência
Relatório gerencial sobre o serviço de alguma equipe do CONTRATO (podendo ser solicitado um relatório com detalhes técnicos e/ou um relatório com informações mais resumidas, em um nível gerencial). O relatório será considerado entregue, mediante a validação e aceite do CONTRATANTE.	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.

14.9.2. Entregas dos Serviços de Gerenciamento de Projetos:

ENTREGAS	PRAZO MÁXIMO DE ENTREGA
Reunião de Status Gerencial contemplando as principais informações sobre os projetos em andamento e encerrados no mês de referência	Até o 10º (décimo) dia do mês subsequente ao mês de referência
Construção de artefatos dos projetos (a ser definido pelo CONTRATANTE): • Plano de gerenciamento de projeto; • Declaração de escopo; • Termo de abertura; • Planilha de riscos; • Cronograma (novo e atualização); • Matriz de comunicação; • Matriz de responsabilidade; • Planilha de desembolsos; • Parecer técnico; • Atas de reunião.	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.
• Apresentação de informações gerenciais de projetos devidamente atualizadas, incluindo os relatórios de acompanhamento de projetos (RAP);	Até as 12h00min de todas as sextas-feiras

14.9.3. Entregas dos Serviços de Consultoria:

ENTREGAS	PRAZO MÁXIMO DE ENTREGA
Prospecção de soluções de mercado visando endereçar alguma necessidade da CONTRATANTE	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.
Elaboração de documento contendo especificações/requisitos técnicos de recursos de hardware, software, pessoas e processos necessários à implantação do projeto;	Em até 60 (sessenta) dias corridos a partir da demanda do CONTRATANTE.
Definição de escopo de assistência técnica, suporte técnico e demais serviços;	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.
Atividades a serem prestadas por fornecedor de produtos ou serviços;	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.
Elaboração de planos de implantação para projetos internos da CONTRATANTE;	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.

Elaboração de pareceres técnicos conforme necessidade da CONTRATANTE	Em até 10 (dez) dias corridos a partir da demanda do CONTRATANTE.

14.9.4. Entregas dos Serviços de Gerenciamento de Conhecimento e Dados:

ENTREGAS	PRAZO DE MÁXIMO DE ENTREGA
Documentos submetidos à base de conhecimento validados, conforme critérios definidos pelo CONTRATANTE.	Em até 5 (cinco) dias úteis após o recebimento do documento.
Elaboração de *dashboards*, painéis entre outras formas de visualizações.	Em até 10 (dez) dias úteis a partir da demanda do CONTRATANTE.
Elaboração de artefatos para equipe a ser especificado, dentre eles: • Processos; • Fluxos; • Modelos de documentos;	Em até 5 (cinco) dias úteis após a solicitação.
Campanha de conscientização seja realizada para todos os colaboradores ou um grupo de colaboradores específico conforme planejamento alinhado com a CONTRATANTE	A cada 6 (seis) meses após a última campanha realizada.
Plano de treinamento contendo a proposta de treinamentos que cada equipe deve realizar.	A cada 6 (seis) meses após o último plano de treinamento entregue.
Relatório de treinamento realizados por cada colaborador do CONTRATO	A cada 1 (um) ano
Cronograma de anual do programa de conscientização contendo o planejamento de todas as ações prevista para realizar durante o ano	A cada 1 (um) ano, até o fim da primeira quinzena de dezembro.
Avaliação de maturidade de tecnologia da informação da organização	A cada 1 (um) ano
Avaliação de maturidade do grupo de resposta a incidentes de segurança	A cada 6 (seis) meses
Avaliação de postura de segurança da organização	A cada 1 (um) ano
Execução de exercício de simulação (*TableTop)*	A cada 1 (um) ano

14.9.5. Entregas dos Serviços de Operações de Segurança da Informação e Cibernética:

ENTREGAS	PRAZO DE MÁXIMO DE ENTREGA
Triagem de Alertas de prioridade CRÍTICA devidamente realizada, de acordo com os padrões definidos pelo CONTRATANTE.	Em até 15 (quinze) minutos após o registro do alerta
Triagem de Alertas de prioridade ALTA devidamente realizada, de acordo com os padrões definidos pelo CONTRATANTE.	Em até 25 (vinte e cinco) minutos após o registro do alerta
Triagem de Alertas de prioridade MÉDIA devidamente realizada, de acordo com os padrões definidos pelo CONTRATANTE.	Em até 45 (quarenta e cinco) minutos após o registro do alerta
Triagem de Alertas de prioridade BAIXA devidamente realizada, de acordo com os padrões definidos pelo CONTRATANTE.	Em até 60 (sessenta) minutos após o registro do alerta

Incidente de Prioridade CRÍTICA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 3 (três) horas após a triagem do Incidente, para o atendimento e resolução deste;
Incidente de Prioridade ALTA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 6 (seis) horas após a triagem do Incidente, para o atendimento e resolução deste;
Incidente de Prioridade MÉDIA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 9 (nove) horas após a triagem do Incidente, para o atendimento e resolução deste;
Incidente de Prioridade BAIXA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 12 (doze) horas após a triagem do Incidente, para o atendimento e resolução deste;
Solicitações de serviços de Prioridade CRÍTICA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 6 (seis) horas após a abertura da solicitação.
Solicitações de serviços de Prioridade ALTA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 12 (doze) horas após a abertura da solicitação.
Solicitações de serviços de Prioridade MÉDIA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 18 (dezoito) horas após a abertura da solicitação.
Solicitações de serviços de Prioridade BAIXA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 24 (vinte e quatro) horas após a abertura da solicitação.
Solicitações de PENTEST/Exercício *RED TEAM* de Prioridade ALTA devidamente atendidos, resolvidos e documentados (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 90 (noventa) dias após a abertura da solicitação.
Solicitações de PENTEST/Exercício *RED TEAM* de Prioridade MÉDIA devidamente atendidos, resolvidos e documentados (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 60 (sessenta) dias após a abertura da solicitação.
Solicitações de PENTEST/Exercício *RED TEAM* de Prioridade BAIXA devidamente atendidos, resolvidos e documentados (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 30 (trinta) dias após a abertura da solicitação.
Solicitações de teste de segurança (análise de vulnerabilidade) devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até o 5 (cinco) dias úteis após a abertura da solicitação.
Elaboração de *baseline* das soluções de segurança	Em até 30 (trinta) dias corridos a partir da demanda do CONTRATANTE.
Realização de *heath check* das soluções de segurança	A cada 3 (três) meses

14.9.6. Entregas dos Serviços de Operações de Combate e Prevenção a Fraude:

ENTREGAS	PRAZO DE MÁXIMO DE ENTREGA
Incidente de Prioridade CRÍTICA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 4 (quatro) horas úteis após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade ALTA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 6 (seis) horas úteis após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade MÉDIA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 8 (oito) horas úteis após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade BAIXA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 12 (doze) horas úteis após o registro do incidente, para o atendimento e resolução deste;
Solicitações de serviços de Prioridade CRÍTICA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 6 (seis) horas úteis após a abertura da solicitação;
Solicitações de serviços de Prioridade ALTA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 12 (doze) horas úteis após a abertura da solicitação;
Solicitações de serviços de Prioridade MÉDIA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 24 (vinte e quatro) horas úteis após a abertura da solicitação;
Solicitações de serviços de Prioridade BAIXA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 36 (trinta e seis) horas úteis após a abertura da solicitação;

14.9.7. Entregas dos Serviços de Operações de Combate e Prevenção à Lavagem de Dinheiro

ENTREGAS	PRAZO DE MÁXIMO DE ENTREGA
Incidente de Prioridade CRÍTICA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 1 (um) dia útil após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade ALTA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 2 (dois) dias úteis após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade MÉDIA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 3 (três) dias úteis após o registro do incidente, para o atendimento e resolução deste;
Incidente de Prioridade BAIXA devidamente atendido e resolvido de acordo com os padrões definidos pelo CONTRATANTE.	Em até 4 (quatro) dias úteis após o registro do incidente, para o atendimento e resolução deste;

Solicitações de serviços de Prioridade CRÍTICA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 1 (um) dia útil após a abertura da solicitação;
Solicitações de serviços de Prioridade ALTA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 5 (cinco) dias úteis após a abertura da solicitação.
Solicitações de serviços de Prioridade MÉDIA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 10 (dez) dias úteis após a abertura da solicitação.
Solicitações de serviços de Prioridade BAIXA devidamente atendidas, resolvidas e documentadas (documentação com evidências da execução), de acordo com os padrões definidos pelo CONTRATANTE.	Em até 15 (quinze) dias úteis após a abertura da solicitação.

14.9.8. Entregas Comuns da Gestão do Contrato:

ENTREGAS	PRAZO DE MÁXIMO DE ENTREGA
Relatório de admissões e desligamentos de profissionais do contrato no mês de referência	Até o 5º (quinto) dia útil do mês subsequente ao do período do relatório
Quadro de profissionais do CONTRATADO devidamente atualizado	Até o 5º (quinto) dia útil do mês subsequente ao do período do relatório

14.10. Janelas para execução dos serviços a seguir:

Janelas dentro das quais as atividades devem estar disponíveis				
Todas as atividades da US - 1 - Serviço de Supervisão de Segurança da Informação e Cibernética	-	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 2 - Serviço de Liderança de Governança de Segurança da Informação	-	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 3 - Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)	-	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 4 - Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)	-	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 5 - Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)	-	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	

Todas as atividades da US - 6 - Serviço de Gerenciamento de Projetos e Melhorias	-	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 7 - Serviço de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)	Perfil I	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
	Perfil II	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 8 - Serviço de Gerenciamento de Dados	-	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 9 - Serviço de Segurança da Informação e Cibernética (Operações de Segurança I)	-	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 10 - Serviço de Segurança da Informação e Cibernética (Operações de Segurança II)	-	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 11 - Serviço de Segurança da Informação e Cibernética (Operações de Segurança III)	-	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 12 - Serviço de Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)	-	24 horas x 7 dias	Atendimento 24x7	Serviço 24x7, podendo ser dividido em 3 turnos de 8 horas, 4 turnos de 6 horas ou 2 turnos de 12 horas, distribuídos nos horários de: 23h às 8h, 07h às 16 e 15h às 00h ou 00h às 6h, 6h às 12h, 12h às 18h e 18h às 00h ou 00h às 12h e 12h às 00h;
Todas as atividades da US - 13 - Serviço de Segurança	Perfil I	24 horas x 7 dias	Atendimento 24x7	Serviço 24x7,

da Informação e Cibernética (Operações Defensivas)				podendo ser dividido em 3 turnos de 8 horas, 4 turnos de 6 horas ou 2 turnos de 12 horas, distribuídos nos horários de: 23h às 8h, 07h às 16 e 15h às 00h ou 00h às 6h, 6h às 12h, 12h às 18h e 18h às 00h ou 00h às 12h e 12h às 00h;
	Perfil II	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
Todas as atividades da US - 14 - Serviço de Segurança da Informação e Cibernética (Operações Ofensivas)	Perfil I	17 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 07h às 00h.	
	Perfil II	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 15 - Serviço de Consultoria	Perfil I	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
	Perfil II	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 16 - Serviço de Operações de Combate e Prevenção a Fraude	Perfil I	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
	Perfil II	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
Todas as atividades da US - 17 - Serviço de Operações de Combate e Prevenção à Lavagem de Dinheiro	Perfil I	8 horas x 5 dias úteis	Nos dias de funcionamento da Direção Geral do Banco, das 08h às 17h.	
	Perfil II	8 horas x 5 dias úteis	Nos dias de funcionamento da	

			Direção Geral do Banco, das 08h às 17h.	

14.11. Na execução dos serviços, deverão ser consideradas as melhores práticas de gestão e qualidade amparadas nos modelos ITIL, COBIT, NBR ISO/IEC 27000 e PMBOK – em suas versões atualizadas;

14.12. Sob a orientação da CONTRATANTE, e no que couber, a CONTRATADA produzirá ou manterá atualizada documentação técnica referente às atividades executadas.