ANEXO IV

PERFIS E QUALIFICAÇÕES DOS PROFISSIONAIS DO CONTRATADO

ATENÇÃO: O Contratado deverá dimensionar uma equipe considerando que férias, ausências legais, atestados médicos e quaisquer outros fatores alheios ao Banco não dispensarão a exigência dos quantitativos mínimos de especialidades exigidos. Ou seja, qualquer ausência programada ou não programada de profissionais do Contratado deverá ser prontamente reposta com o intuito de atender aos quantitativos mínimos solicitados.

1. Os profissionais a serem alocados pelo CONTRATADO deverão ter experiência e conhecimento técnico adequado para a execução dos serviços contratados, atuar de forma presencial nas instalações do CONTRATANTE, devendo ser continuamente treinados e avaliados para assegurar o bom desempenho de suas atribuições além de contribuir para o processo de melhoria contínua e serem contratados sob regime de CLT.

   1.1. O CONTRATANTE poderá, a qualquer tempo, avaliar a possibilidade de atuação remota de unidades de serviço envolvidas no objeto do contrato.

2. A qualificação técnica dos profissionais deve ser comprovada por meio de currículo, que deverá ser obrigatoriamente acompanhado de cópia autenticada ou cópia acompanhada dos originais (quando solicitados pelo CONTRATANTE), da seguinte documentação:

   2.1. CTPS, com declaração/certidão do antigo empregador contendo a descrição das atividades desenvolvidas e o respectivo período de exercício, se experiência sob regime da CLT;

   OU

   2.2. Contrato de prestação de serviços em TI, RAIS do período sem empregados vinculados e declaração/certidão do antigo tomador do serviço contendo a descrição das atividades desenvolvidas e o respectivo período de exercício, se experiência de pessoa jurídica;

   OU

   2.3. Contrato de prestação de serviços em TI e declaração/certidão do antigo tomador do serviço contendo a descrição das atividades desenvolvidas e o respectivo período de exercício, se experiência como autônomo;

   2.4. Diplomas e certificados;

   2.5. Não serão considerados para fins de comprovação da qualificação técnica estágios de aprendizagem e relação de sociedade com empresa de TI. Serão aceitas certificações ou certificados que porventura venham a substituir aqueles que não mais sejam fornecidos.

3. Em caso de impossibilidade de comprovação de experiência profissional através de declaração/certidão do antigo tomador do serviço contendo a descrição das atividades desenvolvidas, fica autorizada a recepção do currículo, desde que excepcionalmente e motivadamente se declare a impossibilidade de apresentação de declaração do empregador detalhando as atividades desenvolvidas.

4. A qualificação dos profissionais que prestarão os serviços poderá ser verificada, a qualquer tempo, pelo CONTRATANTE. Caso os requisitos de qualificação profissional não sejam

atendidos ou sejam considerados insuficientes, o CONTRATADO deverá alocar outro profissional com a qualificação requerida.

5. A CONTRATADA deverá treinar e manter atualizados todos os profissionais responsáveis pela execução das atividades detalhadas no contrato, visando a evolução profissional dos mesmos em função das atualizações tecnológicas que venham a acontecer nesses ambientes;

   5.1. Ao final de cada período de vigência do contrato, a empresa deverá apresentar uma listagem de todos os profissionais treinados (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.

6. O dimensionamento da EQUIPE TÉCNICA necessária para a execução dos serviços, respeitando o mínimo indicado, será de exclusiva responsabilidade do CONTRATADO, devendo ser suficiente para o cumprimento integral dos níveis mínimos de serviço exigidos no Edital.

7. Os membros das equipes deverão atuar exclusivamente na execução dos serviços contratados durante toda a jornada de trabalho, não sendo admitido o compartilhamento de tempo com outras atividades alheias ao objeto do contrato.

8. Para viabilizar a fiscalização pelo CONTRATANTE, as contratações e demissões ocorridas no âmbito do contrato deverão ser informadas de imediato ao CONTRATANTE. Além disso, quando da substituição dos profissionais, o CONTRATADO deverá observar os requisitos de qualificação previstos para cada serviço e deverá encaminhar ao CONTRATANTE documentação que comprove o atendimento a tais requisitos. O CONTRATADO deverá, também, enviar mensalmente um relatório contendo, pelo menos, o quadro geral das especialidades por profissional, os profissionais admitidos e demitidos, a relação dos profissionais ausentes e seus respectivos substitutos.

9. O CONTRATADO deverá garantir a operacionalização dos serviços ora contratados em período de vinte e quatro horas por dia, sete dias por semana (24x7), inclusive sábados, domingos e feriados. Para isso, é obrigatório que o CONTRATADO demonstre e garanta que a EQUIPE TÉCNICA alocada para a execução dos serviços esteja distribuída em turnos, de forma a atender este tipo de regime de trabalho, respeitando-se o previsto na legislação trabalhista e demais preceitos legais, durante toda a execução, até o fim do contrato.

10. A qualquer momento, caso o CONTRATANTE identifique desvios de conduta, não atendimento aos requisitos de qualificação e baixa qualidade técnica no atendimento de demandas por parte dos profissionais do CONTRATADO, este poderá proceder com o cancelamento dos acessos do(s) referido(s) profissional(is) em caráter imediato.

11. Os profissionais alocados nas Unidades de Serviços deverão se adequar aos perfis estabelecidos no edital, conforme Tabela:

Unidade de Serviço	Processo/Serviço	Perfil
US-1	Serviço de Supervisão de Segurança da Informação e Cibernética	**Supervisor Técnico de Execução dos Serviços do Contrato**
US-2	Serviço de Liderança de Governança de Segurança da Informação	**Líder de Governança de Segurança da Informação**
US-3	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)	**Líder de Segurança da Informação (Operações de Segurança)**
US-4	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)	**Líder de Segurança da Informação (Operações Defensivas)**
US-5	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)	**Líder de Segurança da Informação (Operações Ofensivas)**
US-6	Serviço de Gerenciamento de Projetos e Melhorias	**Gerente de Projetos**
US-7	Serviço de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)	**Perfil I - Especialista de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização) - Nível I**
		Perfil II - Especialista de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização) - Nível II
		Perfil III - Especialista de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização) - Nível III
US-8	Serviço de Gerenciamento de Dados	**Especialista de Gerenciamento de Dados**
US-9	Serviço de Segurança da Informação e Cibernética (Operações de Segurança I)	**Especialista de Segurança da Informação e Cibernética (Operações de Segurança)**
US-10	Serviço de Segurança da Informação e Cibernética (Operações de Segurança II)	**Especialista de Segurança da Informação e Cibernética (Operações de Segurança)**
US-11	Serviço de Segurança da Informação e Cibernética (Operações de Segurança III)	**Especialista de Segurança da Informação e Cibernética (Operações de Segurança)**
US-12	Serviço de Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)	**Especialista de Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)**
US-13	Serviço de Segurança da Informação e Cibernética (Operações Defensivas)	**Perfil I - Especialista de Segurança da Informação e Cibernética (Operações Defensiva) - Nível I**
		Perfil II - Especialista de Segurança da Informação e Cibernética (Operações Defensiva) - Nível II
US-14	Serviço de Segurança da Informação e Cibernética (Operações Ofensivas)	**Perfil I - Especialista de Segurança da Informação e Cibernética (Operações Ofensivas) - Nível I**
		Perfil II - Especialista de Segurança da Informação e Cibernética (Operações Ofensivas) - Nível II
US-15	Serviço de Consultoria	**Perfil I – Consultor (a) de Segurança Corporativa**
		Perfil II - Consultor (a) DEVSECOPS
US-16	Serviço de Operações de Combate e Prevenção a Fraude	**Perfil I - Especialista de Operações de Combate e Prevenção a Fraude - Nível I**
		Perfil II - Especialista de Operações de Combate e Prevenção a Fraude - Nível II
		Perfil III - Especialista de Operações de Combate e Prevenção a Fraude - Nível III

US-17	Serviço de Operações de Combate e Prevenção à Lavagem de Dinheiro	**Perfil I - Especialista de Operações de Combate e Prevenção** à Lavagem de Dinheiro **- Nível I**
		Perfil II - Especialista de Operações de Combate e Prevenção à Lavagem de Dinheiro **- Nível II**

As Macroatividades dos serviços estão especificadas no **Anexo II - Especificações dos Serviços**.

12. Perfis e Qualificações dos Profissionais

Os perfis e qualificações dos profissionais que integram os serviços desta contratação estão elencados nos itens seguintes:

12.1. **US - 1: Supervisão de Segurança da Informação e Cibernética**

12.1.1. Qualificações Exigidas:

12.1.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.1.1.2. Experiência comprovada de 05 (cinco) anos no gerenciamento de equipes de segurança da informação ou segurança cibernética;

12.1.1.3. Experiência e conhecimento em Normas ISO, Leis, Auditorias e Conformidade;

12.1.1.4. Experiência com modelos de maturidade, que envolva pelo menos 02 (dois) dos frameworks a seguir: CIS *Control*, *Security Incident Management Maturity Model* (SIM3), NIST *Cybersecurity Framework* (NIST CSF), *Cybersecurity Capability Maturity Model* (C2M2), Mitre ATT&CK, ISO/IEC 27001;

12.1.1.5. Deve possuir, no mínimo, uma das certificações abaixo listadas, dentro do período de validade:

12.1.1.5.1. ISC² *Certified Information System Security Professional* – CISSP; ou

12.1.1.5.2. ISACA *Certified Information Security Manager*® (CISM®); ou

12.1.1.5.3. EC-Council's *Certified Cief Information Security Officer* (C|CISO).

12.2. **US – 2: Liderança de Governança de Segurança da Informação**

12.2.1. Qualificações Exigidas:

12.2.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.2.1.2. Experiência comprovada de 05 (cinco) anos na elaboração de processos, fluxos e procedimentos de equipes e soluções de tecnologia ou segurança da informação;

12.2.1.3. Experiência comprovada de 02 (dois) anos em atividades relacionadas à coordenação ou liderança de equipes;

12.2.1.4. Experiência com modelos de maturidade, que envolva pelo menos 01 (um) dos frameworks a seguir: CIS *Control*, *Security Incident Management Maturity Model* (SIM3), NIST *Cybersecurity Framework* (NIST CSF), *Cybersecurity Capability Maturity Model* (C2M2), Mitre ATT&CK, ISO/IEC 27001;

12.2.1.5. Deve possuir, no mínimo, uma das certificações abaixo listadas, dentro do período de validade:

12.2.1.5.1. *Lead Audit* baseada na ISO/IEC 27001; ou
12.2.1.5.2. *Lead Risk Manager* baseada na ISO/IEC 27005; ou
12.2.1.5.3. *Information Security Management Professional* baseada na ISO/IEC 27001.

12.2.1.6. Deve possuir, no mínimo, 02 (duas) das certificações* a seguir, dentro do período de validade:

12.2.1.6.1. CompTIA Security+;
12.2.1.6.2. CompTIA Cybersecurity Analyst (CySA+);
12.2.1.6.3. COBIT 5;
12.2.1.6.4. Information Security Management Professional baseada na ISO/IEC 27001; ou
12.2.1.6.5. Mile2 Certified Information Systems Security Manager (C)ISSM); ou
12.2.1.6.6. ISC² Systems Security Certified Practitioner (SSCP); ou
12.2.1.6.7. GAQM Certified Information Security Professional (CISP); ou
12.2.1.6.8. Certified Information Systems Auditor (CISA); ou
12.2.1.6.9. ISC² Certified Information System Security Professional – CISSP; ou
12.2.1.6.10. GIAC Information Security Professional Certification (GISP);
12.2.1.6.11. Certified Business Process Associate (CBPA®) ou superior;
12.2.1.6.12. Certified BPM Professional (CBPMPSM);
12.2.1.6.13. Certified Professional in Business Process Management (CPBPM);
12.2.1.6.14. IBM Certified Business Process Analyst;
12.2.1.6.15. Oracle Unified Business Process Management Suite 11g Certified Implementation Specialist;
12.2.1.6.16. BPM 2 fundamentos ou superior.

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.3. **US – 3: Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)**

12.3.1. Qualificações Exigidas:

12.3.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.3.1.2. Experiência comprovada de 05 (cinco) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções de Segurança da Informação de mercado;

12.3.1.3. Experiência comprovada de 02 (dois) anos em atividades relacionadas à coordenação ou liderança de equipes;

12.3.1.4. Deve possuir, no mínimo, uma das certificações abaixo listadas, dentro do período de validade:

12.3.1.4.1. CompTIA Advanced Security Practitioner (CASP+); ou
12.3.1.4.2. ISACA Certified in Risk and Information Systems Control® (CRISC®); ou
12.3.1.4.3. GIAC Information Security Professional Certification (GISP); ou
12.3.1.4.4. Information Security Management Expert baseada na ISO/IEC 27001; ou
12.3.1.4.5. Microsoft 365 Certified: Administrator Expert (MS-100); ou
12.3.1.4.6. Microsoft Certified: Cybersecurity Architect Expert (SC-100).

12.3.1.5. Deve possuir, no mínimo, 02 (duas) das certificações* a seguir, dentro do período de validade:

12.3.1.5.1. CompTIA Security+;
12.3.1.5.2. CompTIA Cybersecurity Analyst (CySA+);
12.3.1.5.3. Security Operations Analyst Associate da *Microsoft (SC-200);*
12.3.1.5.4. Tecnologias de segurança do *Microsoft Azure (AZ-500);*
12.3.1.5.5. EC-Council Certified Network Defender (CND) ou superior*;*
12.3.1.5.6. EC-Council Certified Incident Handler (ECIH);
12.3.1.5.7. EC-Council Certified Threat Intelligence Analyst (CTIA);
12.3.1.5.8. Mile2 Certified Cybersecurity Analyst (C)CSA);
12.3.1.5.9. Mile2 Certified Information Systems Security Manager (C)ISSM);
12.3.1.5.10. ISC² Systems Security Certified Practitioner (SSCP);
12.3.1.5.11. GAQM Certified Information Security Professional (CISP);

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.4. **US – 4: Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)**

12.4.1. Qualificações Exigidas:

12.4.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.4.1.2. Experiência comprovada de 05 (cinco) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração das soluções:

12.4.1.2.1. de Next-Generation Firewall (NGFW) de mercado; e/ou
12.4.1.2.2. de Endpoint detection and response (EDR) de mercado; e/ou
12.4.1.2.3. de Web Application Firewall (WAF) de mercado; e/ou
12.4.1.2.4. de Gestão de Vulnerabilidades de mercado.

12.4.1.3. Experiência comprovada de 02 (dois) anos em atividades relacionadas à coordenação ou liderança de equipes;

12.4.1.4. Deve possuir a certificação Palo Alto *Networks Certified Network Security Engineer* (PCNSE) ou certificação* similar de outros fabricantes de *Next-Generation Firewall* (NGFW);

12.4.1.5. Deve possuir, no mínimo, 02 (duas) das certificações* a seguir, dentro do período de validade:

12.4.1.5.1. EC-Council Certified Network Defender (CND) ou superior;
12.4.1.5.2. Cisco Certified Network Associate Security (CCNA Sec) ou superior;
12.4.1.5.3. CompTIA Security+;
12.4.1.5.4. CompTIA Advanced Security Practitioner (CASP+);
12.4.1.5.5. CompTIA Cybersecurity Analyst (CySA+);
12.4.1.5.6. Palo Alto Networks Certified Security Automation Engineer (PCSAE);
12.4.1.5.7. Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA);
12.4.1.5.8. Palo Alto Networks Micro-Credential Remote Network Administrator (PMRnA);
12.4.1.5.9. F5 BIG-IP Certified Solution Expert – Security;
12.4.1.5.10. Checkpoint Certified Security Expert ou superior;
12.4.1.5.11. Fortinet NSE 8 - Network Security Expert;
12.4.1.5.12. Juniper Networks Certified Internet Professional – Security ou superior;

***Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco**.*

12.4.2. Qualificações Desejáveis:

12.4.2.1. Experiência no uso de *Security Service Edge* (SSE) de mercado;

12.5. **US - 5: Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)**

12.5.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.5.1.2. Experiência comprovada de 05 (cinco) anos na realização de testes de segurança ofensiva em equipamentos de rede, servidores Windows e Linux, aplicações Web e mobile (iOS e Android), elaboração de relatórios técnicos sobre exploração e apresentação de vulnerabilidades;

12.5.1.3. Experiência comprovada de 02 (dois) anos em atividades relacionadas à coordenação ou liderança de equipes;

12.5.1.4. Experiência em pelo menos 02 (dois) dos *frameworks* ou metodologias a seguir: Mitre ATT&CK; ISO/IEC 27001; OWASP *TESTING GUIDE* 3.0 - *The Open Web Application Security Project*; PCI *Penetration Testing Guidance* (*Payment Card Industry*); PTES (*Penetration Testinf Execution Standard*); OSSTMM 3 (*The Open Source Security Testing Methodology Manual*); NIST *Special Publication* 800-115 (*Technical Guide to Information Security Testing and Assessment*); NIST *Special Publication* 800-42 (*Guideline on Network Security Testing*);

12.5.1.5. Deve possuir, no mínimo, uma das certificações abaixo listadas, dentro do período de validade:

12.5.1.5.1. Ofensive Security Certified Professional (OSCP); ou
12.5.1.5.2. Certified Red Team Operator (CRTO); ou
12.5.1.5.3. GIAC Certified Penetration Tester (GPEN);

12.5.1.6. Deve possuir, no mínimo, 02 (duas) das certificações* a seguir, dentro do período de validade:

12.5.1.6.1. CompTIA Security+;
12.5.1.6.2. CompTIA Pentest+;
12.5.1.6.3. EC-Council Certified Ethical Hacker (CEH);
12.5.1.6.4. eLearnSecurity Certified Profesional Penetration Tester (eCCPT);
12.5.1.6.5. eLearnSecurity Mobile Application Penetration Tester (eMAPT);
12.5.1.6.6. eLearnSecurity Web application Penetration Tester (eWPT);
12.5.1.6.7. EC Council Ciertified Penetration Testing Professional (CPENT);
12.5.1.6.8. GIAC Cloud Penetration Tester (GCPN);
12.5.1.6.9. GIAC Web Application Penetration Tester (GWAPT);

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.6. **US – 6: Gerenciamento de Projetos e Melhorias**

12.6.1. Qualificações Exigidas:

12.6.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.6.1.2. Experiência comprovada de 05 (cinco) anos na função de Gerente de Projetos;

12.6.1.3. Experiência em gerenciamento de projetos com base no corpo de conhecimentos do PMI (PMBOK);

12.6.1.4. Experiência no uso das ferramentas de gerenciamento de projetos (exemplos: *IBM Rational Portfolio Manager*, *MS Project*, *Dotproject*, *Open Project* e Primavera);

12.6.1.5. Deve possuir a certificação PMP – *Project Management Professional* do PMI – *Project Management Institute*, em seu período de validade;

12.6.1.6. Deve possuir, no mínimo, uma das certificações* a seguir, dentro do período de validade:

12.6.1.6.1. Professional Agile Leadership (PAL I); ou
12.6.1.6.2. Disciplined Agile® Scrum Master (DASM) Certification; ou
12.6.1.6.3. PMI Agile Certified Practitioner (PMI-ACP); ou
12.6.1.6.4. EXIN Agile Scrum Master; ou
12.6.1.6.5. GAQM Certified Agile Scrum Master (CASM); ou
12.6.1.6.6. Scrum Alliance Certified Scrum Master (CSM);

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.7. **US - 7: Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)**

PERFIL I - Especialista nível I

12.7.1. Qualificações Exigidas:

12.7.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.7.1.2. Experiência comprovada de 01 (um) ano atuando na área de segurança da informação;

12.7.1.3. Deve possuir, no mínimo, uma das certificações* a seguir, dentro do período de validade:

12.7.1.3.1. Fundamentos de Segurança da Informação baseada em *ISO/IEC 27001* ou superior; ou
12.7.1.3.2. *CompTIA Security+* ou superior; ou
12.7.1.3.3. Fundamentos de segurança, conformidade e identidade da Microsoft *(SC-900);* ou
12.7.1.3.4. *EXIN Cyber & IT* Fundamentos *(EXIN CIT)* ou superior; ou
12.7.1.3.5. *ISC² Certified in Cybersecurity (CC)* ou superior.

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

PERFIL II - Especialista nível II

12.7.2. Qualificações Exigidas:

12.7.2.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.7.2.2. Experiência comprovada de 02 (dois) anos atuando na área de segurança da informação;

12.7.2.3. Deve possuir, no mínimo, duas das certificações* a seguir, dentro do período de validade:

12.7.2.3.1. Fundamentos de Segurança da Informação baseada em *ISO/IEC 27001* ou superior; ou
12.7.2.3.2. *CompTIA Security+* ou superior; ou
12.7.2.3.3. Fundamentos de segurança, conformidade e identidade da Microsoft *(SC-900);* ou
12.7.2.3.4. *EXIN Cyber & IT* Fundamentos *(EXIN CIT)* ou superior; ou
12.7.2.3.5. *ISC² Certified in Cybersecurity (CC)* ou superior;
12.7.2.3.6. Mile2 *Certified Cybersecurity Analyst* (C)CSA);
12.7.2.3.7. IBM *Certified Business Process Analyst*

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

PERFIL III - Especialista nível III

12.7.3. Qualificações Exigidas:

12.7.3.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.7.3.2. Experiência comprovada de 02 (dois) anos na elaboração de processos, fluxos e procedimentos de equipes e soluções de tecnologia ou segurança da informação;

12.7.3.3. Deve possuir, no mínimo, 02 (duas) das certificações* a seguir, dentro do período de validade:

12.7.3.3.1. *CompTIA Security+* ou superior; ou
12.7.3.3.2. COBIT 5;
12.7.3.3.3. *Information Security Management Professional* baseada na ISO/IEC 27001; ou
12.7.3.3.4. *Certified Business Process Associate* (CBPA®) ou superior; ou
12.7.3.3.5. *Certified BPM Professional* (CBPMPSM); ou
12.7.3.3.6. *Certified Professional in Business Process Management* (CPBPM); ou
12.7.3.3.7. *IBM Certified Business Process Analyst*; ou
12.7.3.3.8. *Oracle Unified Business Process Management Suite 11g Certified Implementation Specialist*; ou
12.7.3.3.9. BPM 2 fundamentos ou superior.

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.8. **US - 8: Gerenciamento de Dados**

12.8.1. Qualificações Exigidas:

12.8.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;
12.8.1.2. Experiência comprovada de 02 (dois) anos na área de tecnologia com habilidade em *Business Intelligence,* criação de painéis e *Dashboard;*
12.8.1.3. Deve possuir habilidade em 02 (duas) das seguintes ferramentas* de mercado: SAS, IBM *Cloud Pak for Data*, Power BI, Tableau, Qlikview, SQL *Server*, IBM DB2;
12.8.1.4. Deve possuir conhecimento em linguagem SQL;
12.8.1.5. Deve possuir, no mínimo, duas das certificações* a seguir, dentro do período de validade:
12.8.1.5.1. Microsoft Certified: Azure Data Fundamentals (DP-900); ou
12.8.1.5.2. Microsoft Certified: Power Platform Fundamentals (PL-900) ou
12.8.1.5.3. Microsoft Certified: Azure Data Engineer Associate (DP-203); ou
12.8.1.5.4. Microsoft Certified: Azure Database Administrator Associate (DP-300); ou
12.8.1.5.5. Microsoft Certified: Power BI Data Analyst Associate (PL-300); ou
12.8.1.5.6. CompTIA Data+; ou
12.8.1.5.7. SAS Certified Platform Administrator for SAS®9 ou superior; ou
12.8.1.5.8. Tableau Desktop Specialist; AWS Certified Data Analytics - Specialty; ou
12.8.1.5.9. IBM Certified Administrator - Cloud Pak for Data; ou

12.8.1.5.10. IBM Certified Architect - Cloud Pak for Data; ou
12.8.1.5.11. IBM Certified Associate Architect - Cloud Pak for Data; ou
12.8.1.5.12. IBM Certified Solution Architect - Cloud Pak for Data; ou
12.8.1.5.13. IBM Cloud Pak for Data System;

12.9. **US - 9: Segurança da Informação e Cibernética (Operações de Segurança I)**

12.9.1. Qualificações Exigidas:

12.9.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.9.1.2. Experiência comprovada de 02 (dois) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções*****:

12.9.1.2.1. de inteligência de ameaças, inteligência em fontes abertas e automação de segurança de mercado; e/ou
12.9.1.2.2. de correlação de eventos de segurança de mercado;

12.9.1.3. Deve possuir o treinamento oficial das ferramentas RSA Archer e RSA Netwitness ou de soluções similares, a ser avaliado pelo banco;

12.9.1.4. Deve possuir, no mínimo, 02 (duas) das certificações****** a seguir, dentro do período de validade:

12.9.1.4.1. *CompTIA Security+*; ou
12.9.1.4.2. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.9.1.4.3. *RSA Archer Certified Administrator - Specialist*; ou
12.9.1.4.4. *RSA NetWitness Platform Administrator*; ou
12.9.1.4.5. *EC-Council Certified Incident Handler* (ECIH); ou
12.9.1.4.6. *EC-Council Certified Threat Intelligence Analyst* (CTIA); ou
12.9.1.4.7. *Mile2 Certified Threat Intelligence Analyst*; ou
12.9.1.4.8. *Mile2 Certified Cybersecurity Analyst* (C)CSA);

****Pelo menos um dos profissionais deve ter experiência nas soluções/serviços do perfil, as experiências dos profissionais devem ser complementares, não devendo ser centralizada apenas em uma das soluções/serviços.***

*****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

12.10. **US – 10: Segurança da Informação e Cibernética (Operações de Segurança II)**

12.10.1. Qualificações Exigidas

12.10.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.10.1.2. Experiência comprovada de 02 (dois) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções*****:

12.10.1.2.1. de segurança do O365; e/ou
12.10.1.2.2. de *Data Loss Prevention* (DLP) de mercado; e/ou
12.10.1.2.3. de *Cloud Access Security Broker* (CASB) de mercado;

12.10.1.3. Deve possuir, no mínimo, 02 (duas) das certificações****** a seguir, dentro do período de validade:

12.10.1.3.1. *Security Operations Analyst Associate* da Microsoft (SC-200); ou
12.10.1.3.2. Administrador da Proteção de Informações da Microsoft (SC-400); ou
12.10.1.3.3. *CompTIA Security+*; ou
12.10.1.3.4. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.10.1.3.5. *EC-Council Certified Incident Handler* (ECIH);
12.10.1.3.6. Forcepoint DLP: *Data Loss Prevention Administrator Certification*; ou
12.10.1.3.7. *Mile2 Certified Cybersecurity Analyst* (C)CSA);

Pelo menos um dos profissionais deve ter experiência nas soluções/serviços do perfil, as experiências dos profissionais devem ser complementares, não devendo ser centralizada apenas em uma das soluções/serviços.

*****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

12.11. **US - 11: Segurança da Informação e Cibernética (Operações de Segurança III)**

12.11.1. Qualificações Exigidas:

12.11.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.11.1.2. Experiência comprovada de 02 (dois) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções***** ou serviços*****:

12.11.1.2.1. de Gestão de Identidades e Acesso; e/ou
12.11.1.2.2. de diretórios *Active Directory* (AD DS) do Windows no Microsoft Windows Server 2016 ou superior; e/ou
12.11.1.2.3. de certificados do *Active Directory* (AD CS) no Microsoft Windows Server 2016 ou superior;

12.11.1.3. Deve possuir conhecimento de *Hardware Security Module* - HSM de mercado;

12.11.1.4. Deve possuir, no mínimo, 02 (duas) das certificações****** a seguir, dentro do período de validade:

12.11.1.4.1. *CompTIA Security+*; ou
12.11.1.4.2. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.11.1.4.3. *Security Operations Analyst Associate* da Microsoft (SC-200); ou
12.11.1.4.4. Administrador de acesso e identidade da Microsoft (SC-300); ou
12.11.1.4.5. *Thales Luna HSM 5 Professional Certification* ou superior; ou

12.11.1.4.6. *Certified Sailpoint IdentityIQ Associate* ou superior;
12.11.1.4.7. *Certified Identity Professional* (CIDPRO); ou
12.11.1.4.8. *Certified Identity and Access Manager* (CIAM); ou
12.11.1.4.9. *Mile2 Certified Cybersecurity Analyst* (C)CSA);

Pelo menos um dos profissionais deve ter experiência nas soluções/serviços do perfil, as experiências dos profissionais devem ser complementares, não devendo ser centralizada apenas em uma das soluções/serviços.

****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

12.12. **US - 12: Atendimento e Tratamento de Requisições e Resposta a Incidentes (*Security Operations Center*)**

12.12.1. Qualificações Exigidas:

12.12.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.12.1.2. Experiência comprovada de 01 (um) ano atuando na área de segurança da informação;

12.12.1.3. Deve possuir, no mínimo, uma das certificações***** a seguir, dentro do período de validade:

12.12.1.3.1. Fundamentos de Segurança da Informação baseada em ISO/IEC 27001 ou superior; ou
12.12.1.3.2. *CompTIA Security+* ou superior; ou
12.12.1.3.3. Fundamentos de segurança, conformidade e identidade da Microsoft (SC-900); ou
12.12.1.3.4. *EXIN Cyber & IT* Fundamentos (EXIN CIT) ou superior; ou
12.12.1.3.5. *ISC² Certified in Cybersecurity* (CC) ou superior; ou
12.12.1.3.6. *EC-Council Certified SOC Analyst* (CSA); ou
12.12.1.3.7. *EC-Council Certified Incident Handler* (ECIH).

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.13. **US - 13: Segurança da Informação e Cibernética (Operações Defensivas)**

PERFIL I – Especialista nível I

12.13.1. Qualificações Exigidas:

12.13.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.13.1.2. Experiência comprovada de 02 (dois) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções***** ou serviços*****:

12.13.1.2.1. de *Next-Generation Firewall* (NGFW) de mercado; e/ou
12.13.1.2.2. de *Endpoint detection and response* (EDR) de mercado; e/ou
12.13.1.2.3. de *Web Application Firewall* (WAF) de mercado; e/ou

12.13.1.2.4. de Gestão de Vulnerabilidade de mercado.

12.13.1.3. Deve possuir conhecimento em *Security Service Edge* (SSE) de mercado;

12.13.1.4. Deve possuir a certificação Palo Alto *Networks Certified Network Security Administrator* (PCNSA) ou certificação****** similar de outros fabricantes de *Next-Generation Firewall* (NGFW);

12.13.1.5. Deve possuir, no mínimo, uma das certificações****** a seguir, dentro do período de validade:

12.13.1.5.1. *Palo Alto Networks Certified Security Automation Engineer* (PCSAE); ou
12.13.1.5.2. *Palo Alto Networks Certified Detection and Remediation Analyst* (PCDRA); ou
12.13.1.5.3. *Cisco Certified CyberOps Associate* (Cisco COA) ou superior; ou
12.13.1.5.4. *CompTIA Security+*; ou
12.13.1.5.5. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.13.1.5.6. *EC-Council Certified Incident Handler* (ECIH); ou
12.13.1.5.7. *EC-Council Certified Network Defender* (CND) ou superior; ou
12.13.1.5.8. *F5 BIG-IP Certified Administrator* ou superior; ou
12.13.1.5.9. *Fortinet NSE 4 Network Security Professional* ou superior; ou
12.13.1.5.10. *Checkpoint Certified Security Administrator* ou superior;

Pelo menos um dos profissionais deve ter experiência nas soluções/serviços do perfil, as experiências dos profissionais devem ser complementares, não devendo ser centralizada apenas em uma das soluções/serviços.

****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

PERFIL II - Especialista nível II

12.13.2. Qualificações Exigidas:

12.13.2.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.13.2.2. Experiência comprovada de 03 (três) anos na identificação e a análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções***** ou serviços*****:

12.13.2.2.1. de *Next-Generation Firewall* (NGFW) de mercado; e/ou
12.13.2.2.2. de *Endpoint detection and response* (EDR) de mercado; e/ou
12.13.2.2.3. de *Web Application Firewall* (WAF) de mercado; e/ou
12.13.2.2.4. de Gestão de Vulnerabilidade de mercado.

12.13.2.3. Deve possuir conhecimento em *Security Service Edge* (SSE) de mercado;

12.13.2.4. Deve possuir a certificação Palo Alto *Networks Certified Network Security Administrator* (PCNSA) ou certificação****** similar de outros fabricantes de *Next-Generation Firewall* (NGFW);

12.13.2.5. Deve possuir, no mínimo, 02 (duas) das certificações****** a seguir, dentro do período de validade:

12.13.2.5.1. *Palo Alto Networks Certified Security Automation Engineer* (PCSAE); ou
12.13.2.5.2. *Palo Alto Networks Certified Detection and Remediation Analyst* (PCDRA); ou
12.13.2.5.3. *Cisco Certified CyberOps Associate* (Cisco COA) ou superior; ou
12.13.2.5.4. *CompTIA Security+*; ou
12.13.2.5.5. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.13.2.5.6. *EC-Council Certified Incident Handler* (ECIH); ou
12.13.2.5.7. *EC-Council Certified Network Defender* (CND) ou superior; ou
12.13.2.5.8. *F5 BIG-IP Certified Administrator* ou superior; ou
12.13.2.5.9. *Fortinet NSE 4 Network Security Professional* ou superior; ou
12.13.2.5.10. *Checkpoint Certified Security Administrator* ou superior;

Pelo menos um dos profissionais deve ter experiência nas soluções/serviços do perfil, as experiências dos profissionais devem ser complementares, não devendo ser centralizada apenas em uma das soluções/serviços.

*****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

12.14. **US - 14: Segurança da Informação e Cibernética (Operações Ofensivas)**

PERFIL I – Especialista nível I

12.14.1. Qualificações Exigidas:

12.14.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.14.1.2. Experiência comprovada de 02 (dois) anos na realização de testes de segurança ofensiva em equipamentos de rede, servidores Windows e Linux, aplicações Web e mobile (iOS e Android), elaboração de relatórios técnicos sobre exploração e apresentação de vulnerabilidades.

12.14.1.3. Experiência em pelo menos 1 (um) dos *frameworks* ou metodologias a seguir: Mitre ATT&CK; ISO/IEC 27001; OWASP *TESTING GUIDE* 3.0 - *The Open Web Application Security Project*; PCI *Penetration Testing Guidance* (*Payment Card Industry*); PTES (*Penetration Testinf Execution Standard*); OSSTMM 3 (*The Open Source Security Testing Methodology Manual*); NIST *Special Publication* 800-115 (*Technical Guide to Information Security Testing and Assessment*); NIST *Special Publication* 800-42 (*Guideline on Network Security Testing*);

12.14.1.4. Deve possuir, no mínimo, uma das certificações***** a seguir, dentro do período de validade:

12.14.1.4.1. CompTIA Security+; ou

12.14.1.4.2. CompTIA Pentest+; ou
12.14.1.4.3. EXIN Ethical Hacking Foundation (EEHF) ou superior; ou
12.14.1.4.4. EC-Council Certified Ethical Hacker (CEH); ou
12.14.1.4.5. eLearnSecurity Junior Penetration Tester (eJPT); ou
12.14.1.4.6. Desec Certified Penetration Tester (DCPT).

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

PERFIL II - Especialista nível II

12.14.2. Qualificações Exigidas:

12.14.2.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.14.2.2. Experiência comprovada de 03 (três) anos na realização de testes de segurança ofensiva em equipamentos de rede, servidores Windows e Linux, aplicações Web e mobile (iOS e Android), elaboração de relatórios técnicos sobre exploração e apresentação de vulnerabilidades.

12.14.2.3. Experiência em pelo menos 2 (dois) dos *frameworks* ou metodologias a seguir: Mitre ATT&CK; ISO/IEC 27001; OWASP *TESTING GUIDE* 3.0 - *The Open Web Application Security Project*; PCI *Penetration Testing Guidance* (*Payment Card Industry*); PTES (*Penetration Testinf Execution Standard*); OSSTMM 3 (*The Open Source Security Testing Methodology Manual*); NIST *Special Publication* 800-115 (*Technical Guide to Information Security Testing and Assessment*); NIST *Special Publication* 800-42 (*Guideline on Network Security Testing*);

12.14.2.4. Deve possuir, no mínimo, 02 (duas) das certificações***** a seguir, dentro do período de validade:

12.14.2.4.1. CompTIA Security+; ou
12.14.2.4.2. CompTIA Pentest+; ou
12.14.2.4.3. EXIN Ethical Hacking Foundation (EEHF) ou superior; ou
12.14.2.4.4. EC-Council Certified Ethical Hacker (CEH); ou
12.14.2.4.5. eLearnSecurity Junior Penetration Tester (eJPT); ou
12.14.2.4.6. Desec Certified Penetration Tester (DCPT).

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.15. **US-15 Consultoria**

PERFIL I - Consultor (a) de Segurança Corporativa

12.15.1. Qualificações Exigidas

12.15.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.15.1.2. Experiência profissional comprovada de 5 (cinco) anos na área de Tecnologia da Informação e 02 (dois) anos de atuação na identificação e a análise de problemas, bem como administração, gerenciamento,

monitoramento, instalação e configuração de soluções de Segurança da Informação de mercado;

12.15.1.3. Experiência profissional comprovada de 02 (dois) anos de atuação como consultor realizando identificação e análise de problemas, formulação de alternativas, elaboração de editais, implantação de modelos de maturidade e projetos nas especialidades que envolvem conhecimentos relacionados às disciplinas de Segurança da Informação e Cibernética, Combate e Prevenção a Fraude ou Segurança Corporativa;

12.15.1.4. Experiência na implantação e sustentação de modelos de maturidade, que envolva pelo menos 01 (um) dos *frameworks** a seguir: CIS *Control*, *Security Incident Management Maturity Model* (SIM3), NIST *Cybersecurity Framework* (NIST CSF), *Cybersecurity Capability Maturity Model* (C2M2), Mitre ATT&CK, ISO/IEC 27001;

12.15.1.5. Experiência e conhecimento em Normas ISO, Leis, Auditorias e Conformidade;

12.15.1.6. Deve possuir, no mínimo, uma das certificações***** a seguir, dentro do período de validade:

12.15.1.6.1. *Lead Audit* baseada na ISO/IEC 27001; ou
12.15.1.6.2. *Lead Risk Manager* baseado na ISO/IEC 27005; ou
12.15.1.6.3. *Information Security Management Professional* baseada na ISO/IEC 27001;

12.15.1.7. Deve possuir, no mínimo, 02 (duas) das certificações***** a seguir, dentro do período de validade:

12.15.1.7.1. *CompTIA Security+;* ou
12.15.1.7.2. *CompTIA Advanced Security Practitioner (CASP+);* ou
12.15.1.7.3. *CompTIA Cybersecurity Analyst (CySA+);* ou
12.15.1.7.4. *Security Operations Analyst Associate* da Microsoft *(SC-200);* ou
12.15.1.7.5. *Designing Microsoft Azure Infrastructure Solutions (AZ-305);* ou
12.15.1.7.6. Tecnologias de segurança do Microsoft *Azure (AZ-500);* ou
12.15.1.7.7. *EC-Council Certified Network Defender (CND)* ou superior; ou
12.15.1.7.8. *EC-Council Certified Ethical Hacker (CEH);* ou
12.15.1.7.9. *EC-Council Certified Incident Handler (ECIH);* ou
12.15.1.7.10. *Mile2 Certified Cybersecurity Analyst (C)CSA);* ou
12.15.1.7.11. *Mile2 Certified Information Systems Security Manager (C)ISSM);* ou
12.15.1.7.12. *ISC² Systems Security Certified Practitioner (SSCP);* ou
12.15.1.7.13. *GAQM Certified Information Security Professional (CISP);* ou
12.15.1.7.14. *Certified Information Systems Auditor (CISA);* ou
12.15.1.7.15. *ISC² Certified Information System Security Professional – CISSP;* ou
12.15.1.7.16. *GIAC Information Security Professional Certification (GISP);* ou
12.15.1.7.17. *Certified Hacking Forensic Investigator (CHFI);* ou
12.15.1.7.18. *Certified Computer Examiner (CCE);* ou
12.15.1.7.19. *AccessData Certified Examiner (ACE);* ou
12.15.1.7.20. *EnCase™ Certified Examiner (EnCE);* ou
12.15.1.7.21. *GIAC Certified Forensic Analyst (GCFA);* ou
12.15.1.7.22. *Certified Forensic Analyst (CFA);* ou

12.15.1.7.23. Certified Forensic Security Responder (CFSR); ou
12.15.1.7.24. GIAC Network Forensic Analyst (GNFA);

12.15.1.8. Pelo menos dois dos profissionais alocados nesse perfil devem ter:

12.15.1.8.1. Experiência mínima de 02 (dois) anos em atividades de perícia forense computacional englobando atividades de extração de dados, análise forense em ambientes Windows/Linux, rede e *mobiles*.

12.15.1.8.2. Especialização em Forense Computacional ou pelo menos uma das certificações a seguir:

12.15.1.8.2.1. *Certified Hacking Forensic Investigator* (CHFI); ou
12.15.1.8.2.2. *Certified Computer Examiner* (CCE); ou
12.15.1.8.2.3. *AccessData Certified Examiner* (ACE); ou
12.15.1.8.2.4. *EnCase™ Certified Examiner* (EnCE); ou
12.15.1.8.2.5. *GIAC Certified Forensic Analyst* (GCFA); ou
12.15.1.8.2.6. *Certified Forensic Analyst* (CFA); ou
12.15.1.8.2.7. *Certified Forensic Security Responder* (CFSR); ou
12.15.1.8.2.8. *GIAC Network Forensic Analyst* (GNFA);

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.15.2. Qualificações Desejáveis:

12.15.2.1. Desejável especialização em Segurança da Informação e/ou Redes de Computadores e/ou Forense Computacional e/ou Nuvem.

PERFIL II – Consultor (a) DEVSECOPS

12.15.3. Qualificações Exigidas

12.15.3.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.15.3.2. Experiência profissional comprovada de 5 (cinco) anos na área de Tecnologia da Informação e 02 (dois) anos de atuação em identificação e análise de problemas, formulação de alternativas e seu detalhamento nas especialidades que envolvem conhecimento relacionados à disciplina Desenvolvimento ágil e Seguro e/ou operações segura;

12.15.3.3. Experiência e conhecimento em Normas ISO, Leis, Auditorias e Conformidade;

12.15.3.4. Deve possuir conhecimentos em pelo menos 02 (duas) linguagens***** de programação entre as linguagens a seguir: C#, Python, *BashShell*, PHP, C++, Java, *JavaScript*, *PowerShell*;

12.15.3.5. Deve possuir, no mínimo, uma das certificações***** a seguir, dentro do período de validade:

12.15.3.5.1. *EC-Council Cetified DevSecOps Engineer*; ou
12.15.3.5.2. *Designing and Implementing Microsoft DevOps Solutions* (AZ-400);

12.15.3.6. Deve possuir, no mínimo, 02 (duas) das certificações***** a seguir, dentro do período de validade:

12.15.3.6.1. CompTIA Security+; ou
12.15.3.6.2. Designing Microsoft Azure Infrastructure Solutions (AZ-305); ou
12.15.3.6.3. EC-Council Cetified Application Security Engineer - .NET (CASE); ou
12.15.3.6.4. EC-Council Cetified Application Security Engineer - Java (CASE); ou
12.15.3.6.5. EXIN DevSecOps Manager; ou
12.15.3.6.6. Certified Secure Web Application Engineer da Mile2 (C)SWAE); ou
12.15.3.6.7. ISC² Certified Secure Software Lifecycle Professional (CSSLP); ou
12.15.3.6.8. ISC² Systems Security Certified Practitioner (SSCP); ou
12.15.3.6.9. GAQM Certified DevOps Master (CDM).

****Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.***

12.15.4. Qualificações Desejáveis:

12.15.4.1. Desejável especialização em Segurança da Informação e/ou Engenharia de Software

12.16. **US-16 Operações de Combate e Prevenção a Fraude**

PERFIL I – Especialista nível I

12.16.1. Qualificações Exigidas

12.16.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.16.1.2. Experiência comprovada de 01 (um) ano atuando na área de tecnologia da informação;

12.16.2. Qualificações Desejáveis:

12.16.2.1. Treinamento em ferramentas de *Business Intelligence BI* (IBM QRadar, IBM *Cloud Pak for Data*, SAS *Enterprise Guide*, SAS *Visual Analytics* e *Power* BI);

12.16.2.2. Conhecimento da linguagem SQL.

12.16.2.3. Desejável possuir uma das certificações a seguir, dentro do período de validade:

12.16.2.3.1. Fundamentos de Segurança da Informação baseada em ISO/IEC 27001 ou superior; ou
12.16.2.3.2. *CompTIA Security+* ou superior; ou
12.16.2.3.3. Fundamentos de segurança, conformidade e identidade da Microsoft (SC-900); ou
12.16.2.3.4. *EXIN Cyber & IT* Fundamentos (EXIN CIT) ou superior; ou
12.16.2.3.5. *ISC² Certified in Cybersecurity* (CC) ou superior; ou
12.16.2.3.6. *EC-Council Certified SOC Analyst* (CSA); ou
12.16.2.3.7. EC-Council Certified Incident Handler (ECIH);
12.16.2.3.8. Microsoft Certified: Azure Data Fundamentals (DP-900).

PERFIL II - Especialista nível II

12.16.3. Qualificações Exigidas

12.16.3.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.16.3.2. Experiência comprovada de 02 (dois) anos na identificação e na análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções de segurança da informação ou combate e prevenção a fraudes;

12.16.3.3. Conhecimento da linguagem SQL.

12.16.3.4. Deve possuir, no mínimo, uma das certificações***** a seguir, dentro do período de validade:

12.16.3.4.1. Fundamentos de Segurança da Informação baseada em ISO/IEC 27001 ou superior; ou
12.16.3.4.2. *CompTIA Security+* ou superior; ou
12.16.3.4.3. Fundamentos de segurança, conformidade e identidade da Microsoft (SC-900); ou
12.16.3.4.4. *EXIN Cyber & IT* Fundamentos (EXIN CIT) ou superior; ou
12.16.3.4.5. *ISC² Certified in Cybersecurity* (CC) ou superior; ou
12.16.3.4.6. *EC-Council Certified SOC Analyst* (CSA); ou
12.16.3.4.7. EC-Council Certified Incident Handler (ECIH);
12.16.3.4.8. Microsoft Certified: Azure Data Fundamentals (DP-900).

***Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco**.*

12.16.4. Qualificações Desejáveis:

12.16.4.1. Conhecimento desejável em ferramentas de Business *Intelligence BI* (por exemplo: IBM QRadar, SAS *Enterprise Guide*, SAS *Visual Analytics* e *Power* BI);

PERFIL III - Especialista nível III

12.16.5. Qualificações Exigidas

12.16.5.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.16.5.2. Experiência comprovada de 02 (dois) anos na identificação e na análise de problemas, formulação de alternativas de solução e seus detalhamentos, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções de combate e prevenção a fraudes;

12.16.5.3. Conhecimento da linguagem SQL.

12.16.5.4. Deve possuir, no mínimo, 02 (duas) das certificações***** a seguir, dentro do período de validade, ou uma das certificações* a seguir além de especialização em Forense Computacional:

12.16.5.4.1. *CompTIA Security+*; ou
12.16.5.4.2. *CompTIA Cybersecurity Analyst* (CySA+); ou
12.16.5.4.3. *EC-Council Certified Incident Handler* (ECIH); ou
12.16.5.4.4. *Mile2 Certified Cybersecurity Analyst* (C)CSA); ou
12.16.5.4.5. *Security Operations Analyst Associate* da Microsoft (SC-200); ou
12.16.5.4.6. *Certified Hacking Forensic Investigator* (CHFI); ou
12.16.5.4.7. *Certified Forensic Analyst* (CFA); ou
12.16.5.4.8. *ISACA's Certified Cybersecurity Operations Analyst* (CCOA); ou
12.16.5.4.9. *EC-Council Certified Security Specialist*.

***Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco**.*

12.16.6. Qualificações Desejáveis:

12.16.6.1. Conhecimento desejável em ferramentas de Business *Intelligence BI* (por exemplo: IBM QRadar, SAS *Enterprise Guide*, SAS *Visual Analytics* e *Power* BI);

12.17. **US-17 Operações de Combate e Prevenção à Lavagem de Dinheiro**

PERFIL I – Especialista nível I

12.17.1. Qualificações Exigidas

12.17.1.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação e seus correlatos, ou Estatística e seus correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos ou Estatística e seus correlatos;

12.17.1.2. Experiência comprovada de 02 (dois) anos na área de Análise de Dados, com habilidade em *Business Intelligence*, processos ETL e criação de *Dashboard*;

12.17.1.3. Deve possuir habilidade em 02 (duas) das seguintes ferramentas de mercado: SAS, IBM Cloud Pak for Data, Power BI, Tableau, Qlikview, SQL Server, IBM DB2;

12.17.1.4. Deve possuir conhecimento em linguagem Python e SQL;

12.17.1.5. Deve possuir, no mínimo, 01 (uma) das certificações***** a seguir, dentro do período de validade, ou uma das certificações* a seguir além de especialização em Forense Computacional:

12.17.1.5.1. Microsoft Certified: Azure Data Engineer Associate (DP-203); ou
12.17.1.5.2. Microsoft Certified: Azure Database Administrator Associate (DP-300); ou
12.17.1.5.3. Microsoft Certified: Power BI Data Analyst Associate (PL-300); ou
12.17.1.5.4. CompTIA Data+; ou
12.17.1.5.5. SAS Certified Platform Administrator for SAS®9 ou superior; ou
12.17.1.5.6. Tableau Desktop Specialist; AWS Certified Data Analytics - Specialty; ou
12.17.1.5.7. IBM Certified Administrator - Cloud Pak for Data; ou

12.17.1.5.8. IBM Certified Architect - Cloud Pak for Data; ou
12.17.1.5.9. IBM Certified Associate Architect - Cloud Pak for Data; ou
12.17.1.5.10. IBM Certified Solution Architect - Cloud Pak for Data; ou
12.17.1.5.11. IBM Cloud Pak for Data System;

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.17.2. Qualificações Desejáveis:

12.17.2.1. Conhecimentos em ferramenta SAS (por exemplo: SAS Enterprise Guide e SAS Visual Analytics);
12.17.2.2. Conhecimento em ambiente de aprendizado de máquina (Machine Learning) e algoritmos preditivos;
12.17.2.3. Conhecimento em algoritmos de Machine Learning;
12.17.2.4. Conhecimento em estatística;

PERFIL II – Especialista nível II

12.17.3. Qualificações Exigidas

12.17.3.1. Formação Acadêmica: Curso Superior completo em Tecnologia da Informação e seus correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

12.17.3.2. Experiência comprovada de 02 (dois) anos na área de Tecnologia da Informação, com habilidade em banco de dados relacional;

12.17.3.3. Deve possuir habilidade em 02 (duas) das seguintes ferramentas de mercado: SQL Server, PostgreSQL, MySQL, IBM DB2, Oracle, SAS, IBM Cloud Pak for Data, IBM Datastage;

12.17.3.4. Deve possuir conhecimento em linguagem SQL;

12.17.3.5. Deve possuir, no mínimo, 01 (uma) das certificações* a seguir, dentro do período de validade, ou uma das certificações* a seguir além de especialização em Forense Computacional:

12.17.3.5.1. Microsoft Certified: Azure Data Engineer Associate (DP-203); ou
12.17.3.5.2. Microsoft Certified: Azure Database Administrator Associate (DP-300); ou
12.17.3.5.3. Microsoft Certified: Power BI Data Analyst Associate (PL-300); ou
12.17.3.5.4. CompTIA Data+; ou
12.17.3.5.5. AWS Certified Data Engineer – Associate; ou
12.17.3.5.6. AWS Certified Big Data – Specialty; ou
12.17.3.5.7. AWS Certified Data Analytics - Specialty; ou
12.17.3.5.8. IBM Certified Data Architect – Big Data; ou
12.17.3.5.9. IBM Certified Architect - Cloud Pak for Data; ou
12.17.3.5.10. IBM Certified Associate Architect - Cloud Pak for Data; ou
12.17.3.5.11. IBM Certified Solution Architect - Cloud Pak for Data; ou
12.17.3.5.12. Oracle Database Administration Certified Professional; ou
12.17.3.5.13. Certified PostgreSQL DBA(CPSDBA); ou
12.17.3.5.14. MySQL Database Administration; ou
12.17.3.5.15. SAS Certified Platform Administrator for SAS®9 ou superior; ou
12.17.3.5.16. Tableau Desktop Specialist.

Outras certificações similares que não estejam na relação disponível devem ser avaliadas pelo Banco.

12.17.4. Qualificações Desejáveis:

12.17.4.1. Conhecimentos em ferramenta SAS (por exemplo: SAS Enterprise Guide e SAS Visual Analytics);
12.17.4.2. Conhecimento em linguagens de programação Python;
12.17.4.3. Conhecimento desejável em Big Data/ Data Lake;
12.17.4.4. Conhecimento desejável em mineração de dados;