Objeto	Fase	Entrega	Tipo de Avaliação	Quantidade Consultores	Horas estimadas por atividades (Análises/Reuniões/recomendações)	Horas estimadas (E*F)	Prazo estimado (em Dias)	Observações
- Identificar e criar a execução dos processos de segurança indicados no âmbito do SERPRO. Frente Processos - Avaliação e diagnosticar os GAPS de segurança interna de ambientes de segurança de mercado relacionados abaixo com fases aplicadas a equipe de operação e dono do processo: **01- Processo de Governança de identidade e acesso** **02- Processo de Gestão de acesso** **03- Processo de Gestão de usuários privilegiados** **04- Processo de Análise dinâmica de vulnerabilidade** **05- Processo de Análises táticas do código fonte**	**Entrevistas-Coleta [1]**	EP0- Seleção dos Frameworks de referência para avaliação do referido processo	Geral	2	10	20		
		EP1- Registros e Realização de Entrevistas e workshops	Geral	2	4	8		
		EP2- Eventuais riscos e pontos de atenção identificados na fase inicial.	Geral	1	4	4		
	Análise e Diagnóstico [2]	AP1 - Identificação de oportunidade de melhorias do processo	Geral	1	4	4		
		AP2 - Lista de riscos identificados	Geral	2	4	8		
		AP3 - Diagnóstico da aderência e maturidade dos processos em consonância ao Cobit 2019, ITIL 4, Scrum, Kanban e melhores práticas de mercado	Geral	2	10	20		
		AP4 - Diagnóstico da execução de cada processo analisado em relação aos modelos e processos da Empresa, seja por sistema ou geral conforme indicado	Geral	2	10	20		
		AP5 - Lista de riscos identificados ao analisar a execução dos processos	Geral	2	4	8		
		Avaliar o Grau de maturidade dos processos, ou procedimentos internos frente aos modelos de referrência do mercado	Geral	2	12	24		
	Recomendações [3]	RP1 - Apresentação final para as equipes e lideranças	Geral	2	4	8		
		RP2 - Recomendações de implantação de novos processos ou adaptações dos processos quanto à conformidade com modelo de referência Cobit 2019, ITIL 4, Scrum, Kanban e melhores práticas de mercado	Geral	2	10	20		
		RP3 - Definição dos fatores que influenciarão a priorização das recomendações (ex: complexidade de implementação, custos de implementação, grau de benefício para o negócio, dependência de outros projetos e legados)	Geral	2	4	8		
		RP4 - Definição do plano de mitigação para os riscos identificados	Geral	2	4	8		
		RP5 - Recomendações e ações com base na coleta de informações e diagnóstico realizado nos processos que suportam as aplicações infraestrutura e sistemas	Geral	2	4	8		
		RP8 - Consolidação final dos relatórios técnicos e plano de ação com as recomendações distribuídas ao longo do tempo e esforço	Geral	2	4	8		
		RP9 - Fornecer a relatório de lacunas (relatório Gap análise), diagnostico, grau de maturidade e aderência, e falhas nos processos e suas integrações, bem como recomendações para mitigá-las, por processo avaliado, bem como para cada sistema quanto ao processo avaliados e plano de ação	Geral	3	20	60		
Total de Horas por Processo	236							
Total de Horas Geral (5 processos)	1180							

[1] ● Avaliação das documentações e entendimento dos processos operacionais vitais das áreas de sustentação e desenvolvimento de software (processos de gestão de incidentes, gestão de mudanças, gestão de crises, implantação em produção, esteira de testes, etc);
● Condução das entrevistas técnicas com os responsáveis das áreas de desenvolvimento e sustentação;
● Disparo das pesquisa eletrônica visando acelerar a coleta de informações sobre os sistemas e processos;
● Avaliação dos planos e processos de continuidade operacional: Backup, recuperação de desastres, testes de chaveamento de ambientes, etc.
● Coletar informações sobre os mecanismos de governança de TI relacionadas a processos de gestão existentes, estrutura organizacional, papéis e responsabilidades, competências, KPIs, estrutura de comitês, metodologias e etc.

[2] ● Determinação dos riscos que podem afetar a operação juntamente com o grau de impacto. Serão utilizados como métodos revisões da documentação, técnicas de coleta de informações e brainstorming;
● Análise das informações coletadas através de entrevistas e pesquisa eletrônica;
● Análise dos processos de desenvolvimento, sustentação e continuidade operacional dos sistemas suportados pelo SERPRO, incluindo o levantamento dos controles e proteções existentes que poderiam prevenir ou minimizar a ocorrência das ameaças / eventos relacionadas;
● Análise de resiliência (alto nível) dos ambientes que hospedam as aplicações.

[3] ● Definir os fatores que influenciarão a priorização das recomendações (ex: complexidade de implementação, custos de implementação, grau de benefício para o negócio, dependência de outros projetos e legados, etc.);
● Definir o plano de mitigação para os riscos identificados;
● Desenvolver as recomendações e ações com base na coleta de informações e diagnóstico realizado nos processos que suportam as aplicações infraestrutura e sistemas;
● Analisar em alto-nível de esforço para realização das recomendações identificadas;
● Consolidação final dos relatórios técnicos e plano de ação com as recomendações distribuídas ao longo do tempo e esforço