FUNDAÇÃO DE PREVIDÊNCIA
COMPLEMENTAR DO
SERVIDOR PÚBLICO FEDERAL
DO PODER EXECUTIVO

Funpresp

CONTRATO Nº 5/2024

Processo nº 03750.010105.000005/2021-48

CONTRATO DE PRESTAÇÃO DE SERVIÇO DE SEGURANÇA CIBERNÉTICA, QUE ENTRE SI CELEBRAM A FUNDAÇÃO DE PREVIDENCIA COMPLEMENTAR DO SERVIDOR PÚBLICO FEDERAL DO PODER EXECUTIVO– FUNPRESP-EXE E A INTEROP INFORMÁTICA LTDA.

A FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO FEDERAL DO PODER EXECUTIVO – FUNPRESP-EXE, com sede no Edifício Corporate Financial Center - SCN - Quadra 02 – Bloco A – 2º Andar – Salas 201 a 204 – Brasília – DF – CEP: 70712-900, inscrita no CNPJ sob o nº 17.312.597/0001-02, doravante denominada **CONTRATANTE**, neste ato representada por seu Diretor-Presidente, o **Sr. CÍCERO RAFAEL BARROS DIAS**, brasileiro, casado, portador da cédula de identidade nº 97.002.492.914– SSP/CE, inscrito no CPF sob o nº 629.731.263-04, cargo para o qual foi nomeado mediante a Resolução do Conselho Deliberativo nº 607, de 10 de novembro de 2023 e por seu Diretor de Administração, o **Sr. CLEITON DOS SANTOS ARAÚJO**, brasileiro, solteiro, portador da cédula de identidade nº 1.675.172, expedida pela SSP/DF, inscrito no CPF sob o nº 851.631.201- 15, cargo para o qual foi nomeado mediante a Resolução do Conselho Deliberativo nº 452, de 06 de outubro de 2021, ambos residentes e domiciliados em Brasília/DF, na forma da competência contida no Anexo I da Política de Alçadas da **CONTRATANTE**, e de outro lado a empresa **INTEROP INFORMÁTICA LTDA,** inscrita no CNPJ sob o nº 86.703.337/0001-80, estabelecida na Rua General João Manoel, nº 50, 5º Andar, Centro Histórico, Porto Alegre/RS, CEP: 90.010-30, daqui por diante designada **CONTRATADA**, neste ato representada pelo sócio o **Sr. SÓCRATES SLONGO**, brasileiro, divorciado, portador da cédula de identidade nº 5.036.293.016, expedida pela SSP/RS e do CPF nº 512.537.040-15, residente e domiciliado em Porto Alegre/RS, resolvem celebrar o presente Contrato, em conformidade com o que consta do Processo Administrativo nº 03750.010105.000005/2021-48, referente ao Pregão Eletrônico nº 90001/2024, nos termos da Lei nº 13.303, de 30 de junho de 2016 e do Regulamento Interno de Licitações e Contratações da Funpresp-Exe, aprovado pelo Conselho Deliberativo na 127ª Reunião Ordinária, de 22 de setembro de 2023, por meio da Resolução nº 595, aplicando-se, subsidiariamente, a Lei nº 14.133, de 1º de abril de 2021, demais legislações correlatas e mediante as cláusulas e condições seguintes:

1. CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O objeto do presente instrumento é a contratação de serviços gerenciados de Segurança Cibernética pelo período de 36 meses, na forma de serviços continuados, que serão prestados nas condições estabelecidas no Termo de Referência, anexo deste instrumento.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

1.3.1. Item 3 - SERVIÇO DE TESTES DE INVASÃO;

CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - 36 MESES						
Grupo	Item	Descrição do Serviço	Quantidade	Unidade	Valor Unitário	Valor Total
3	1	SERVIÇO DE TESTES DE INVASÃO	36	mês	R$ 22.777,77	R$ 819.999,72

2. CLÁUSULA SEGUNDA – DA VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato será de 36 (trinta e seis) meses a contar da data da sua assinatura, podendo ser prorrogada por prazo não superior a 60 (sessenta) meses, contados a partir da celebração do contrato nos termos do art. 71 da Lei nº 13.303/2016 e da Seção IV do Regulamento Interno de Licitações e Contratações da Funpresp-Exe, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

2.1.1. Os serviços tenham sido prestados regularmente;

2.1.2. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.1.3. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.4. Seja juntada justificativa e motivo, por escrito, de que a CONTRATANTE mantém interesse na realização do serviço;

2.1.5. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a CONTRATANTE;

2.1.6. Haja manifestação expressa da contratada informando o interesse na prorrogação;

2.1.7. Seja comprovado que o contratado mantém as condições iniciais de habilitação.

3. CLÁUSULA TERCEIRA – DO PREÇO

3.1. A CONTRATANTE pagará à CONTRATADA o valor mensal de R$ 22.777,77 (vinte e dois mil, setecentos e setenta e sete reais e setenta e sete centavos)perfazendo o valor global de R$ 819.999,72 (oitocentos e dezenove mil novecentos e noventa e nove reais e setenta e dois centavos), para a prestação dos serviços de SERVIÇO DE TESTES DE INVASÃO, conforme descrito no subitem 1.3 deste instrumento.

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA - DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes da contratação para o corrente exercício correrão à conta dos recursos constantes do orçamento de 2024 – Despesas do Plano de Gestão Administrativa, aprovado na 129ª reunião ordinária do Conselho Deliberativo, de 17 de novembro de 2023, na Ação Orçamentária – Tecnologia da Informação, Item – Infraestrutura, Segurança e Suporte de TI – Cibersegurança.

4.2. Nos exercícios seguintes as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA - DO PAGAMENTO

5.1. O prazo e condições para pagamento à CONTRATADA encontram-se definidos no Termo de Referência, anexo deste instrumento e na Seção III do Regulamento Interno de Licitações e Contratações da Funpresp-Exe.

6. CLÁUSULA SEXTA - DO REAJUSTE

6.1. As regras acerca do reajuste do valor contratual são as estabelecidas no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA – DA GARANTIA DE EXECUÇÃO

7.1. A garantia de execução está prevista no Termo de Referência, anexo I deste Contrato, e nos artigos 147 ao 155 do Regulamento Interno de Licitações e Contratações da Funpresp-Exe.

8. CLÁUSULA OITAVA - DO REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O regime de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo desse instrumento.

9. CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo desse instrumento.

10. CLÁUSULA DÉCIMA – DAS SANÇÕES ADMINISTRATIVAS.

10.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo desse instrumento, e na Seção X do Regulamento Interno de Licitações e Contratações da Funpresp-Exe.

11. CLÁUSULA DÉCIMA PRIMEIRA – DA RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido nos termos dos artigos 142 a 146 do Regulamento Interno de Licitações e Contratações da Funpresp-Exe.

12. CLÁUSULA DÉCIMA SEGUNDA – DAS VEDAÇÕES

12.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13. CLÁUSULA DÉCIMA TERCEIRA – DA PROTEÇÃO DE DADOS

13.1. Caso a CONTRATADA, no decorrer da prestação de serviços, tenha acesso a dados pessoais, deverá respeitar as regras editadas pela Autoridade Nacional de Proteção de Dados ("ANPD") no tocante ao armazenamento e tratamento de referidos dados e informações, sem prejuízo do estrito respeito à Lei nº 12.965 de 2014 ("Marco Civil da Internet"), Decreto nº 8.771 de 2016 ("Regulamento do Marco Civil da Internet"), bem como quaisquer outras leis ou normas relativas à proteção de dados pessoais que vierem a ser promulgadas ou entrarem em vigor no curso da vigência deste Contrato, em especial a Lei nº 13.709 de 2018 ("Lei Geral de Proteção de Dados Pessoais") e dos normativos internos da Funpresp-Exe quanto ao tema.

14. CLÁUSULA DÉCIMA QUARTA – DAS ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina pelos artigos 72 e 81 da Lei nº 13.303/2016 e na Seção V do Regulamento Interno de Licitações e Contratos da Funpresp-Exe.

14.2. A CONTRATADA, desde que haja acordo entre as partes, poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15. CLÁUSULA DÉCIMA QUINTA - DA VALIDADE DA ASSINATURA ELETRÔNICA

15.1. As partes desde já acordam que o presente instrumento e os demais documentos correlatos poderão ser assinados eletronicamente por meio de plataforma que assegure a sua autoria e integridade, reconhecendo desde já a sua validade jurídica, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

16. CLÁUSULA DÉCIMA SEXTA - DA CONDUTA ANTICORRUPÇÃO

16.1. A CONTRATADA declara conduzir suas atividades em conformidade com a Lei 12.846/2013 "Lei Anticorrupção" ou eventual legislação posterior/complementar à referida Lei, assim como quaisquer normativo relacionado a sua aplicabilidade, emitido por órgão regulador brasileiro e/ou órgão do Governo Federal, e atesta neste ato que seus conselheiros, diretores, colaboradores, sócios, agentes ou quaisquer pessoas agindo em seu nome, não realizaram e se comprometem a não realizar atos de suborno ou promessa de suborno, fraude à licitação, financiamento à prática de atos ilícitos ou quaisquer "atos lesivos" assim descritos na Lei Anticorrupção e normativos a ela relacionados, seja em benefício próprio e, ainda, em eventual benefício da CONTRATANTE ("Conduta Anticorrupção"), bem como que se compromete a monitorar todas as pessoas listadas acima, tendo em vista que possui conhecimento que a CONTRATANTE adota abordagem de zero tolerância em relação a atos de corrupção.

16.2. A CONTRATADA deverá informar à CONTRATANTE, oportunamente e por escrito, sobre a ocorrência de qualquer violação à Lei Anticorrupção de que tenha ciência em relação às suas atividades, bem como atos que envolvam seu relacionamento com a CONTRATANTE. Esta é uma obrigação permanente e deverá perdurar até o término da relação.

16.3. Em caso de descoberta da prática de ato de corrupção praticado pela CONTRATADA, suas coligadas, conselheiros, diretores, empregados, colaboradores, agentes ou qualquer pessoa agindo em seu nome, sejam em benefício próprio, da CONTRATADA, poderá ocorrer imediato rompimento da presente relação, sem prejuízo do direito da CONTRATANTE à retenção de valores e regresso em caso de sanções aplicadas decorrentes da Lei Anticorrupção, bem como a reparação de eventuais danos causados à CONTRATANTE.

17. CLÁUSULA DÉCIMA SÉTIMA - DOS CASOS OMISSOS

17.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 13.303, de 2016, no Regulamento Interno de Licitações e Contratos da Funpresp-Exe, presente no endereço: https://www.funpresp.com.br/wp-content/uploads/2023/10/Regulamento-Interno-de-Licitacoes-e-Contratacoes.pdf , e demais normas federais aplicáveis e, subsidiariamente, regras e princípios de direito privado.

18. **CLÁUSULA DÉCIMA OITAVA - DA PUBLICAÇÃO**

18.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União.

19. **CLÁUSULA DÉCIMA NONA - DO FORO**

19.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Circunscrição Especial Judiciária de Brasília do Tribunal de Justiça do Distrito Federal e Territórios.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado, que, depois de lido e achado em ordem, vai assinado pelos contraentes e duas testemunhas, em formato digital.

Brasília/DF, _____, de abril de 2024.

Pela Contratante:
CÍCERO RAFAEL BARROS DIAS
DIRETOR PRESIDENTE

CLEITON DOS SANTOS ARAÚJO
DIRETOR DE ADMINISTRAÇÃO

Pela Contratada:
SÓCRATES SLONGO
INTEROP

Testemunhas:
FABIANE DE SOUSA DUMONT
IBSEN NAEZIO ALVES AGUIAR
Analistas de Previdência Complementar

Anexo I do Contrato 05/2024 - Termo de Referência (0141399).

FUNDAÇÃO DE PREVIDÊNCIA
COMPLEMENTAR DO
SERVIDOR PÚBLICO FEDERAL
DO PODER EXECUTIVO

Funpresp

TERMO DE REFERÊNCIA - TR

1. **OBJETO**

1.1. Contratação de serviços gerenciados de Segurança Cibernética pelo período de 36 meses, na forma de serviços continuados, conforme especificações técnicas estabelecidas neste instrumento e anexos.

2. **DETALHAMENTO DO OBJETO**

2.1. A solução de serviços gerenciados de Segurança Cibernética é composta de itens de serviço integrados e contínuos de segurança da informação que englobam instalação, ação e monitoramento remoto da infraestrutura de TI da CONTRATANTE, por meio da constante coleta e análise, em tempo real, dos logs de segurança gerados pelos ativos de rede; resposta a incidentes de segurança, de modo a minimizar consequências e proteger as informações críticas; provimento e gerenciamento remoto dos ativos de segurança, por meio de ajustes de configuração que reduzem a probabilidade de ataques.

GRUPO	ITEM	DESCRIÇÃO	DETALHAMENTO	QTD	UN
1	1	**SERVIÇO DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES**	Visa sustentar e operar todo o parque tecnológico da Funpresp-Exe (hardware e software) no tocante a Segurança da Informação, por meio de um catalogo de serviço pré-estabelecido pela Funpresp-Exe, descrito em anexo do presente termo de referência, porém não se limitando apenas a este anexo. Espera-se que a CONTRATADA também defina e realize, de forma periódica, ações proativas de acompanhamento de todo parque, a fim de mantê-lo sempre estável, disponível e confiável sobre as questões de Segurança da Informação.	36	MES
	2	**SERVIÇO DE GESTÃO DE VULNERABILIDADES**	Visa de forma proativa e recorrente, identificar possíveis vulnerabilidades de Segurança da Informação na infraestrutura e nas aplicações da Funpresp-Exe, a fim de evitar que ataques cibernéticos direcionados à Funpresp-Exe obtenham sucesso explorando possíveis vulnerabilidades.	36	MES
	3	**SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS**	Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à Funpresp-Exe por meio de fornecimento de solução de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura da Funpresp-Exe. Devem gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.	36	MES
	4	**SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA**	Visa analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados se descobriu que de fato era um ataque à Funpresp-Exe, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um Cyber Security Operations Center - CSOC, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.	36	MES
	5	**SERVIÇO DE PROTEÇÃO DE TRÁFEGO DE BORDA**	Visa o fornecimento e a manutenção pela CONTRATADA, durante toda a vigência do contrato, de equipamentos firewall NGFW de perímetro, junto com todo o serviço aqui descrito, que suporte as demandas atuais e futuras da organização, possibilitando o crescimento e amadurecimento tecnológico da Funpresp-Exe	36	MES
	6	**SERVIÇO DE INTELIGÊNCIA APLICADA À SEGURANÇA**	Visa fazer buscas contínuas em Deep e Dark web sobre dados relacionados à Funpresp-Exe, sendo discutidas ou até mesmo comercializadas de forma ilegal.	36	MES
	7	**SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO**	Visa conscientizar todos os usuários do parque tecnológico do CONTRATANTE sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificar proativamente os usuários que seriam vetores de ataques, e tornando-os elegíveis para um programa de capacitação interna sobre boas práticas de segurança da informação no ambiente corporativo do CONTRATANTE, e proativamente protegendo o ambiente do CONTRATANTE de forma eficiente contra e-mails e mensagens instantâneas com vírus, spams, phishing, botnets, ameaças avançadas, vazamento de informações, entre outros.	36	MES
2	1	**SERVIÇOS TÉCNICOS ESPECIALIZADOS**	Para eventuais necessidades de novas implementações e/ou suporte de soluções de segurança da informação, durante o período de execução do contrato, que não conflitam ou pertençam ao objeto já estabelecido no presente termo de referência. Ou seja, necessariamente tem de ser uma nova necessidade não prevista ou imaginada no momento da contratação, porém identificada como necessária durante a execução do contrato. Esta contratação se dará por demanda em regime de banco de horas.	1440	HORAS
3	1	**SERVIÇO DE TESTES DE INVASÃO**	Visa identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas especificas para tentar obter acesso não autorizado e privilegiado aos ativos e informações	36	MES

3. **ESPECIFICAÇÕES TÉCNICAS**

3.1. Conforme Especificações Técnicas - Anexos 1 ao 17.

4. **CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS**

4.1. Os interessados poderão participar da presente licitação, ofertando proposta para qualquer um os Grupos, desde que atendidas as exigências do Edital e de seus Anexos, bem como ao que se segue:

4.1.1. Um mesmo licitante ou sua subsidiária/controlada não poderá ser contratado para os Grupos 01 e 03, dada a necessidade de autonomia entre os serviços.

4.1.2. Caso a mesma licitante se consagre vencedora dos grupos 01 e 03, somente será aceita sua proposta para o grupo 01 e será desclassificada para o grupo 03, em face da inviabilidade de execução de ambos os serviços pela mesma empresa.

5. **ENQUADRAMENTO DO OBJETO**

5.1. O objeto a ser adquirido enquadra-se na categoria de bens e serviços comuns, de que tratam o Regulamento Interno de Licitações e Contratos da Funpresp-Exe, por possuir padrões de desempenho e características gerais e específicas, usualmente encontradas no mercado.

( )	Serviço não continuado
(x)	Serviço continuado SEM dedicação exclusiva de mão de obra
( )	Serviço continuado COM dedicação exclusiva de mão de obra
( )	Material de consumo
( )	Material permanente / equipamento

6. **JUSTIFICATIVA DA CONTRATAÇÃO**

6.1. **Contextualização e Justificativa da Contratação**

6.1.1. A Funpresp-Exe necessita de um amplo conjunto de recursos computacionais para viabilizar a adequada gestão dos planos de previdência complementar dos servidores do Poder Executivo e do Poder Legislativo. Nos últimos anos, a entidade cresceu de forma acelerada, alcançando 100 mil participantes, divididos em dois planos (ExecPrev e LegisPrev).

6.1.2. Adicionalmente, as reformas legislativas em andamento podem ocasionar um crescimento expressivo no número de participantes nos próximos anos, seja pela aceleração da migração de regime dos atuais servidores, seja pela eventual possibilidade de que a Funpresp-Exe poderá assumir a gestão de Planos de Previdência Complementar de entes subnacionais, com a criação de novos Planos. Assim, é vital investir em tecnologias apropriadas para fortalecer e ampliar a capacidade de processamento e gestão da informação, de forma autônoma, escalável, confiável e segura.

6.1.3. A atual preocupação global sobre ameaças cibernéticas tem feito com que gestores passem cada vez mais a se preocupar com o risco cibernético nas corporações. Em recente publicação* do Fórum Econômico Mundial, é possível concluir, de fato, que os riscos tecnológicos são uma grande preocupação a nível global. A matriz abaixo, extraída dessa publicação, mostra que a preocupação com relação à segurança da informação está focada basicamente em 3 (três pilares): Cyberattacks, Data fraud or theft e Information infrastructure breakdown.

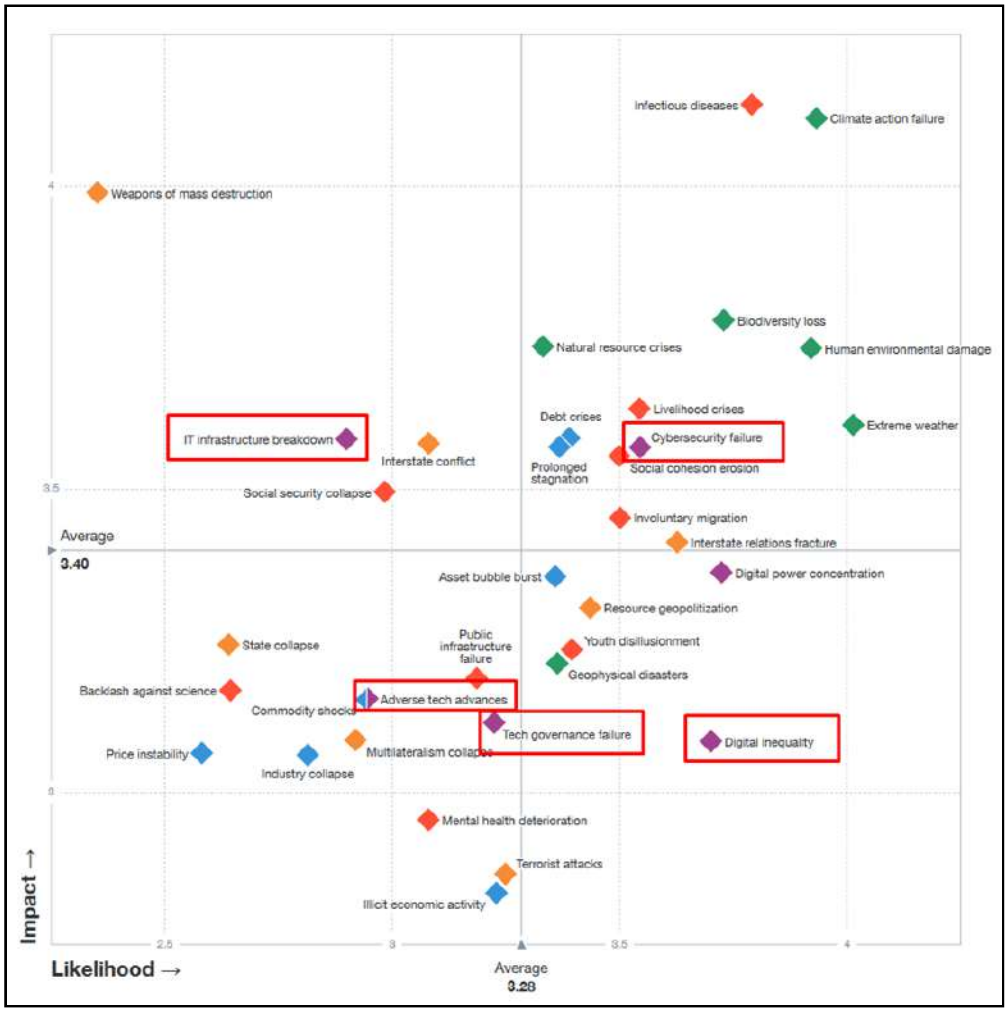

Figura 1 Global Risks Landscape. FONTE: The Global Risks Report 2021 https://www.weforum.org/reports/the-global-risks-report-2021

Figura 2 Global Risks Landscape. FONTE: The Global Risks Report 2021 https://www.weforum.org/reports/the-global-risks-report-2021

6.1.4. Com base nessa análise, a Funpresp-Exe entende como necessária a contratação de empresa especializada em prover serviços de operação e monitoramento de segurança da informação para atuar no ambiente corporativo, de forma padronizada, tendo como principais atividades:

- Operar e monitorar a solução de segurança da informação da Funpresp-Exe, com capacidade de alertas e ações coordenadas.
- Detectar potenciais intrusos na Rede da Funpresp-Exe.
- Fornecer e administrar solução de correlação dos eventos de segurança da informação, ocorridos em todo a Funpresp-Exe, gerando base de conhecimento.
- Fazer a análise de vulnerabilidades do ambiente da Funpresp-Exe.
- Controlar os acessos individualizados aos serviços de internet.
- Realizar testes de invasão controlados para auditar os controles implementados.
- Administrar a disponibilidade da infraestrutura de rede que suporta os serviços disponibilizados pela Rede da Funpresp-Exe (portais, correio eletrônico, sistemas corporativos, entre outros).

6.1.5. Os Serviços Gerenciados de Segurança têm por objetivo o aumento de maturidade e o correto dimensionamento da equipe para o tratamento de incidentes de Segurança da Informação e ações de prevenção e de melhoria de segurança do ambiente computacional da Funpresp-Exe.

6.1.6. Desta forma, justifica-se a contratação para proteger dois relevantes ativos intangíveis da Funpresp-Exe, que são as informações armazenadas e trafegadas na rede e a sua imagem como instituição confiável de previdência complementar perante à sociedade.

7. REQUISITOS GERAIS DOS SERVIÇOS

7.1. Requisitos de Negócio

7.1.1. No âmbito da Funpresp-Exe, a Gerência de Tecnologia e Informação (GETIC) é responsável por planejar, desenvolver, implantar e manter os sistemas de informação, seja com recursos computacionais internos ou externos. Além disso, é de sua responsabilidade propor políticas e também planejar, coordenar, supervisionar e orientar normativamente as atividades de gestão dos recursos de tecnologia da informação e segurança da informação institucional.

7.1.2. A solução de segurança a ser contratada visa, de forma contínua, suportar o gerenciamento, monitoramento, tratamento e proteção aos incidentes de segurança do ambiente tecnológico da Funpresp-Exe de acordo com as seguintes necessidades de negócio:

7.1.2.1. Prover suporte, monitoramento, operação e gestão de serviços de segurança por meio de soluções próprias ou da Funpresp-Exe;

7.1.2.2. Prover suporte e administração de ativos e tecnologias de segurança conforme soluções existentes no ambiente de segurança da Funpresp-Exe;

7.1.2.3. Sustentar e operar todo o parque tecnológico através de um catálogo de serviços pré-estabelecidos pela Funpresp-Exe por meio do SOC;

7.1.2.4. Documentar e realizar a gestão de respostas aos incidentes de segurança;

7.1.2.5. Elaborar planos, programas, workshops, pesquisas e questionários de segurança da informação voltados para melhoria e conscientização de usuários em geral da Funpresp-Exe;

7.1.2.6. Prover serviços de inteligência aplicados à segurança em busca de informações pertinentes à Funpresp-Exe;

7.1.2.7. Responder a ataques de forma imediata colocando os responsáveis da Funpresp-Exe a par da situação de vulnerabilidades, ameaças ou riscos graves à infraestrutura da Funpresp-Exe;

7.1.2.8. Auxiliar nos problemas relacionados à segurança de ENDPOINTS externos no qual a Funpresp-Exe faz comunicação;

7.1.2.9. Monitorar vulnerabilidades e ameaças em tempo real no que tange à segurança dos ativos de rede e comunicação da Funpresp-Exe;

7.1.2.10. Garantir a aplicação da Política de Segurança da Informação e Comunicações (POSIC) da Funpresp-Exe;

7.1.2.11. Prover serviços de operação e gerenciamento de segurança integrados e customizados, capazes de fornecer os níveis de serviço exigidos em contrato em termos de efetividade e prazo;

7.1.2.12. Manter a continuidade dos serviços de segurança atualmente prestados na infraestrutura de TI;

7.1.2.13. Executar as políticas de segurança da informação, públicas, privadas (uso interno da Funpresp-Exe) e restritas (uso por um grupo restrito)

7.1.2.14. Apoiar as equipes de infraestrutura, sistemas, banco e administração de dados na implantação da esteira de integração continua do DevOPs, no que couber;

7.1.2.15. Elaborar planos e programas de segurança da informação e acesso a dados ou recursos de TI;

7.1.2.16. Proteger a integridade e a confiabilidade dos sistemas de informação contra incidentes de segurança;

7.1.2.17. Minimizar a duração e o impacto de uma eventual violação de segurança dos ativos e informações através de ações imediatas de contenção e erradicação de ameaças;

7.1.2.18. Aplicar a inteligência de proteção contra ataques cibernéticos;

7.1.2.19. Agir proativamente para reduzir a interrupção de serviços em parte ou como um todo, ainda que algum evento de segurança não tenha impactado o usuário final;

7.2. **Requisitos de Capacitação**

7.2.1. Não haverá necessidade de capacitação da equipe de TI da Funpresp-Exe, pois trata-se de contratação de Serviços Especializados prestados por profissionais especializados com experiência comprovada na realização das atividades.

7.3. **Requisitos Legais**

7.3.1. Lei n.º13.303, de 30/06/2016;

7.3.2. Regulamento Interno de Licitações e Contratos da Funpresp-Exe;

7.3.3. Decreto federal nº 10.024/19, de 20/09/2019 e demais normas pertinentes.

7.4. **Requisitos de Manutenção**

7.4.1. A CONTRATADA deverá disponibilizar canal para abertura de chamados para suporte e manutenção via Web, e-mail ou telefone;

7.4.2. Os serviços de atendimento técnico, suporte e manutenção dos equipamentos e softwares disponibilizados são de exclusiva responsabilidade da CONTRATADA.

7.5. **Requisitos Temporais**

7.5.1. Os Serviços Gerenciados de Segurança devem ser entregues nos prazos máximos estabelecidos na tabela abaixo, a partir da abertura da especifica OS de implantação do item de serviço, por parte do gestor do contrato.

7.5.2. Para a conclusão de um item de serviço é necessário que todas as atividades referentes a todos os subitens itens de serviço que a compõem sejam concluídas, incluindo a emissão do recebimento definitivo de todos os itens de serviço que a compõem.

7.5.3. Antes do início de cada implantação de serviço deve haver reunião de alinhamento do respectivo serviço.

7.5.4. Poderá haver, no máximo, paralelismo de **04 (quatro)** itens de serviço em implantação a critério da CONTRATANTE.

ITEM	DESCRIÇÃO	PRAZO DE IMPLANTAÇÃO EM DIAS ÚTEIS APÓS OS
1	SERVIÇO DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES	30
2	SERVIÇO DE GESTÃO DE VULNERABILIDADE	30
3	SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICO	30
4	SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA	30
5	SERVIÇO DE PROTEÇÃO DE TRÁFEGO DE BORDA	30
6	SERVIÇO DE INTELIGÊNCIA APLICADA À SEGURANÇA	60
7	SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO	30
8	SERVIÇOS TÉCNICOS ESPECIALIZADOS	30
9	SERVIÇO DE TESTES DE INVASÃO	30

Tabela 1 - Prazos de implantação

7.6. **Requisitos de Segurança e Privacidade**

7.6.1. O serviços de implantação e o gerenciamento centralizado das soluções deverão estar compatíveis com os normativos de segurança da informação vigentes no Brasil, considerando a Lei Nº 13.709, de 14 de agosto de 2018, LGPD.

7.7. **Requisitos Sociais, Ambientais e Culturais**

7.7.1. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada;

7.7.2. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

7.8. **Requisitos de Arquitetura Tecnológica**

7.8.1. Todos os produtos e softwares necessários à correta prestação dos Serviços Especializados para serem instalados na infraestrutura da Contratante devem estar nos padrões adotados pela Contratante.

7.8.2. A CONTRATADA do serviço deverá disponibilizar espaço físico com características de Datacenter profissional, que aumentem sua disponibilidade, resiliência e segurança de acesso, com as seguintes características:

7.8.2.1. Circuito fechado de TV, com monitoramento 24 x 7;

7.8.2.2. Rede elétrica estabilizada, com entradas de alimentação, grupos geradores e sistema de baterias redundantes;

7.8.2.3. Sistema de climatização redundante, com controle de temperatura;

7.8.2.4. Piso suspenso;

7.8.2.5. Sistema de detecção de fumaça, umidade e de combate a incêndio;

7.8.3. A CONTRATADA será a responsável por fornecer todas as ferramentas e licenças para a prestação do serviço, exceto quando explicitamente definido;

7.8.4. Toda infraestrutura necessária para correta execução das atividades dos Serviços de forma remota, como por exemplo acesso à Internet, estação de trabalho, sistema operacional etc, será de responsabilidade e provimento da Contratada.

7.8.5. A comunicação entre os ambientes da Funpresp-Exe e CONTRATADA será feita por VPN site-to-site, não sendo necessário link dedicado.

7.9. **Requisitos de Projeto e de Implementação**

7.9.1. A CONTRATADA deverá desenvolver e apresentar cronograma de implantação, além de definir estratégia de implantação em conjunto com a equipe técnica da Funpresp-Exe.

7.10. **Requisitos de de Implantação**

7.10.1. É responsabilidade da CONTRATADA o levantamento de todas as informações necessárias para implantação de cada serviço, incluindo topologia e configuração atual, processos de trabalho em execução e locais de execução dos serviços.

7.10.2. Em até 10 (dez) dias após abertura da OS devem ser elaborados e apresentados a CONTRATANTE documentos de Projeto Executivo do serviço, contendo, no mínimo, as seguintes informações:

a) Descrição detalhada dos equipamentos e softwares de cada serviço.

b) Descrição da topologia lógica e física de equipamentos e softwares da solução proposta.

c) Cronograma detalhado de execução as atividades.

d) Indicação de técnicos responsáveis pela implantação dos serviços.

e) Descrição dos fluxos de tráfego de rede referentes a cada serviço.

f) Mapeamento dos ativos referentes a cada serviço, inclusive aqueles de propriedade da CONTRATANTE.

g) Condições de rollback no caso de falha de migração tecnológica.

h) Descrição da estratégia da migração e/ou colocação em produção das configurações atuais para o ambiente proposto.

i) Descrição das necessidades de memória, armazenamento e processador para os elementos a serem instalados em ambiente virtualizado da CONTRATANTE.

7.10.3. A apresentação do Projeto Executivo é condição obrigatória e sua aprovação necessária para o início da instalação e configuração de equipamentos e softwares que compõe cada um dos serviços.

7.10.4. A CONTRATADA deverá apresentar também os prazos de aquisição, entrega e instalação dos equipamentos e softwares, execução de serviços e informações para o estabelecimento da VPN entre os ambientes;

7.10.5. Deverá ser criada matriz de responsabilidades definindo as equipes e limites de atuação da equipe técnica da CONTRATADA e da Funpresp-Exe. Vale atentar que a atividade referente à montagem do ambiente tecnológico é de responsabilidade da equipe técnica da CONTRATADA, ficando a cargo da Funpresp-Exe a passagem de informações e concessões iniciais de acesso.

7.11. **Requisitos de Garantia**

7.11.1. A CONTRATADA prestará garantia contratual no montante de 5% (cinco por cento) do valor global do contrato, tendo seu valor atualizado nas mesmas condições nele estabelecidas, no prazo de até 10 (dez) dias úteis a contar da convocação pela Funpresp-Exe, optando por uma das seguintes modalidades de garantia previstas na lei 13.303/2016:

a) Caução em dinheiro;

b) Seguro-garantia, emitido por instituição credenciada na Superintendência de Seguros Privados - Susep; ou

c) Fiança bancária, emitida por banco ou instituição financeira devidamente autorizada a operar no país pelo Banco Central do Brasil.

7.11.2. Demais regras constarão da minuta do contrato.

7.12. **Requisitos de Experiência Profissional**

7.12.1. Os Serviços Gerenciados de Segurança devem ser prestados por profissionais com a experiência profissional descrita nesse Termo de Referência.

7.13. **Requisitos de Formação de Equipe**

7.13.1. Todos os profissionais devem possuir formação de nível superior, graduação ou pós-graduação em Tecnologia da Informação ou áreas correlatas com carga-horária mínima de 360 (trezentos e sessenta) horas, com diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

7.13.2. Todos os profissionais devem demonstrar habilidades comportamentais relacionadas à proatividade, capacidade de trabalho em equipe, capacidade de expressão e comunicação, flexibilidade, capacidade de tomada de decisão e capacidade de seguir processos e normas;

7.13.3. Os pré-requisitos para os profissionais são necessários para executar com qualidade todas as atividades previstas nos serviços contratados, para lidar com a complexidade das soluções utilizadas pela CONTRATANTE, e para atuar em um mercado dinâmico, de alta criticidade e muito sensível e dependente da qualidade dos produtos de software;

7.13.4. Todos os profissionais que integram os grupos apresentados abaixo devem, obrigatoriamente, compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal

serviço;

7.13.5. **Não será exigida a dedicação exclusiva de profissionais na gestão e execução dos serviços demandados pela CONTRATANTE**;

7.13.6. É de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para a entrega do serviço, sem que haja impacto no nível de serviço estabelecido no tópico NÍVEIS MÍNIMOS DE SERVIÇO do presente termo de referência;

7.13.7. A documentação comprobatória das qualificações exigidas deve ser apresentada para cada profissional nas ocasiões mencionadas nesse Termo de Referência ou, quando não mencionado, em até três dias úteis antes da efetiva prestação do serviço pelo profissional;

7.13.8. Para a correta execução dos serviços, a CONTRATADA deverá disponibilizar responsável (PREPOSTO) com formação em qualquer disciplina afeita à Engenharia ou à Tecnologia da Informação e as seguintes atribuições específicas:

7.13.8.1. Coordenar atividades de infraestrutura entre as equipes técnicas da CONTRATADA para o atendimento das necessidades encaminhadas pela equipe técnica/gerencial de TIC da Funpresp-Exe;

7.13.8.2. Receber as demandas dos serviços relativas à área de infraestrutura e providenciar a execução e alocação de recursos de trabalho;

7.13.8.3. Providenciar a automatização de atividades de operação e a execução de tarefas agendadas, sempre que possível;

7.13.8.4. Coordenar ações conjuntas de infraestrutura com a área de Segurança da Informação, no atendimento das melhores práticas de segurança;

7.13.8.5. Coordenar a implantação das melhorias solicitadas pela equipe técnica da Funpresp-Exe, através das aberturas de chamados no sistema informatizado disponibilizado pela CONTRATADA;

7.13.9. Para a implantação dos serviços, as CONTRATADAS deverão disponibilizar recurso com o perfil de **GERENTE DE PROJETOS.**

7.13.10. Adicionalmente, a CONTRATADA para o **Grupo 1** deverá manter as seguintes TORRES DE OPERAÇÃO:

7.13.10.1. Para o Grupo 1, item 1 - SERVIÇO DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES: A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade para executar o processo de resposta a incidente de segurança do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o grupo solucionador com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir todas as certificações indicadas no respectivo perfil, ou equivalentes.

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de segurança de perímetro II	. CompTIA Advanced Security Practitioner certificate.	
Analista de segurança de Endpoint	. CompTIA Security+; . Linux LPIC 3.	

7.13.10.2. Para o Grupo 1, item 2 - SERVIÇO DE GESTÃO DE VULNERABILIDADES: Este grupo deverá ser exclusivo para trabalhar nos SERVIÇOS DE GESTÃO DE VULNERABILIDADES, não podendo os profissionais pertencentes a este grupo ser compartilhados e/ou atuar nos demais serviços descritos no objeto do presente termo de referência. Contudo, não é requisito que tal equipe seja para atendimento exclusivo da CONTRATANTE. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de gestão de vulnerabilidades do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o grupo com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir todas as certificações indicadas no respectivo perfil, ou equivalentes.

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	CompTIA Cybersecurity Analyst (CySA+)	
Analista de Segurança Linux	Linux LPIC 3.	
Analista de Segurança Windows	Microsoft 365 Certified: Security Administrator Associate	

7.13.10.3. Para o Grupo 1, item 3 - SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS: Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podendo os profissionais pertencentes a este grupo ser compartilhados ou atuar nos demais serviços descritos no objeto do presente termo de referência. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o grupo com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir todas as certificações indicadas no respectivo perfil, ou equivalentes.

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	CompTIA Cybersecurity Analyst (CySA+)	
Analista de Segurança III	Certified Ethical Hacker; Linux LPIC 3.	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

7.13.10.4. Para o Grupo 1, item 4 - SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA: Este grupo deverá ser exclusivo para trabalhar nos SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA, não podendo os profissionais pertencentes a este grupo ser compartilhados ou atuar nos demais serviços descritos no objeto do presente termo de referência. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade, para executar o processo de resposta a incidente de segurança do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o grupo com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir todas as certificações indicadas no respectivo perfil, ou equivalentes.

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	CompTIA Cybersecurity Analyst (CySA+)	
Analista de Segurança III	Certified Ethical Hacker; Linux LPIC 3.	Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

7.13.11. A CONTRATADA para o **Grupo 3** deverá apresentar equipe para a prestação de serviço de teste de invasão com as seguintes qualificações básicas:

7.13.11.1. Para o Grupo 3, item 1 - SERVIÇO DE TESTES DE INVASÃO: Obrigatório ao menos uma certificação por perfil.

Perfis	Certificações	Descrição
Analista de Teste de Invasão	EC-Concil Licensed Penetration Tester – LPT ou IACRB Certified Expert Penetration Tester – CEPT ou GIAC Exploit Researcher and Advanced Penetration Tester – GXPN Offensive Security Certified Professional – OSCP Certified Ethical Hacker – CEH Certified Penetration Testing Professional - CPENT CompTIA PenTest+	Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação.

7.14. **Requisitos de Metodologia de Trabalho**

7.14.1. Os chamados para atendimento da(s) CONTRATADA(s) poderão ser abertos apenas pelos contatos autorizados pela equipe técnica da Funpresp-Exe;

7.14.2. O fornecimento dos equipamentos e demais requisitos necessários à adequada execução dos serviços, tais como ferramentas de software, licenças, certificados digitais, dentre outros, são de responsabilidade da CONTRATADA;

7.15. **Requisitos de Segurança da Informação**

7.15.1. Os Serviços Especializados devem ser prestados observando a Política de Gestão e Segurança da Informação da Funpresp-Exe.

8. **OUTROS REQUISITOS APLICÁVEIS**

8.1. Todos os dados coletados são de propriedade da Funpresp-Exe e nenhum dado poderá ser utilizado sem expressa autorização.

8.2. Os requisitos gerais, definem os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA. A seguir, as especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto.

8.3. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

8.4. **Canais de Comunicação**

8.4.1. Para abertura de solicitações, a CONTRATADA deverá disponibilizar 02 (dois) tipos de canais de comunicação a saber:

ITEM	GRUPO DE TECNOLOGIA	CLASSIFICAÇÃO
1	E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 1
2	Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 2

8.4.2. Independente do canal de comunicação utilizado pelo CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM, ou seja, caso a abertura de chamado se dê por via e-mail, este deve ser tratado na mesma ferramenta disponibilizada para a abertura direta.

8.4.3. Para requisições de serviço de severidade alta, ou seja, que exige uma velocidade de comunicação e atendimento maior, a CONTRATADA deverá disponibilizar canal para escalação de chamados, disponível 24x7.

8.4.4. Para um eventual cenário de crise, ou seja, onde o negócio do CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

8.4.5. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL, com certificado digital emitido em nome da CONTRATADA.

8.4.6. A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.

8.4.7. A sala virtual ainda deve ter capacidade para até 10 (dez) pessoas da CONTRATANTE simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

8.4.8. A CONTRATADA deverá prover um portal web para acompanhamento de indicadores da execução do contrato, com o intuito de permitir o acompanhamento a qualquer tempo pela equipe de segurança da CONTRATANTE, além da facilitação na tomada de decisões por parte da equipe técnica desta.

8.5. **Horário de Atendimento**

8.5.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

8.6. **Entrega de Serviços**

8.6.1. Deverá ser disponibilizada equipe para acompanhamento de entregas através de reuniões para avaliação e acompanhamento da execução contrato, de periodicidade mínima mensal. Estas reuniões devem servir para identificação das necessidades da CONTRATANTE onde deverão ser apontados problemas recorrentes ou pontuais que estejam impactando o serviço ou a qualidade da execução do contrato;

8.6.1.1. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato;

8.6.2. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas;

8.6.3. Todos os entregáveis do contrato são acompanhados pelo preposto da CONTRATADA ou pessoa por ele indicada – desde SLA de atendimento a relatórios, a fim de garantir a conformidade e cadência correta estabelecida;

8.6.4. Deverá ser feito o acompanhamento do cronograma de faturamento mensal do contrato;

8.6.5. Deverá manter a matriz de comunicação atualizada dos dois lados do contrato, ou seja, os contatos da CONTRATANTE e da CONTRATADA que irão tratar o andamento da gestão do serviço, inclusive em situações específicas ou de escalação. Entende-se como escalação os problemas em que a tratativa não foi eficaz e efetiva ou foi atendida fora do tempo acordado, fazendo com que a CONTRATANTE eleve o tema para um nível hierárquico superior da CONTRATATADA. Exemplos:

I - Falta de atuação de algum time especifico;

II - Falta de resposta à um e-mail, chamado, questionamentos do cliente;

III - Falta de solução à um problema sinalizado pelo cliente;

IV - Chamado em aberto, não atendido dentro do SLA acordado em contrato;

V - Insatisfação do cliente sobre um entregável como relatório, boletins, atuação, postura de recursos ou times.

8.6.6. As soluções providas pela CONTRATADA deverão ter acesso de leitura para a equipe técnica da CONTRATANTE.

8.7. **Gestão de Catálogo de Serviço do Ambiente de Segurança da Informação**

8.7.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da Funpresp-Exe, se definiu previamente um catálogo de serviços, o qual obrigatoriamente a CONTRATADA deverá ser capaz de entregar. Tal definição pode ser consultada através do anexo 11 no presente termo de referência.

8.7.2. É de responsabilidade da CONTRATADA manter, atualizar, revisar, os serviços disponíveis para cada grupo de serviço. As responsabilidades da CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.

8.7.3. O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma on line para a CONTRATANTE, onde o mesmo poderá consultar a qualquer tempo os serviços disponíveis. Este sistema deve ser o mesmo descrito no tópico SOBRE O SISTEMA DE ITSM A SER UTILIZADO, no presente termo de referência, e obviamente deve seguir os mesmos requisitos técnicos supracitados.

8.7.4. Apesar de já existir uma definição prévia dos serviços a serem ofertados pela CONTRATADA, através do catálogo de serviço do anexo 11 no presente termo de referência, a CONTRATANTE a qualquer tempo poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço.

8.7.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços, seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à CONTRATANTE tal ação.

8.8. **Modalidade de Atendimento**

8.8.1. A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada nas dependências da CONTRATADA, obedecendo, obrigatoriamente, os critérios estabelecidos para execução do mesmo, conforme previstos no presente termo de referência.

8.8.2. Eventualmente a CONTRATANTE poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado em suas dependências físicas, situada no endereço SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900

8.8.3. Os atendimentos, nas dependências da CONTRATANTE ou remotos, referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados.

8.9. **Acessibilidade e Confidencialidade**

8.9.1. Para garantir a qualidade e disponibilidade dos serviços remoto, deverá entre o CONTRATANTE e o CSOC da CONTRATADA, será estabelecida conexão VPN site-to-site entre a CONTRATADA e a Funpresp-Exe para a prestação dos serviços.

8.9.2. Os equipamentos no ambiente da CONTRATADA devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

8.9.3. A CONTRATADA deve assinar e entregar ao CONTRATANTE na data de reunião de início do contrato termo de confidencialidade e sigilo, conforme modelo contido no ANEXO 14 - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO. Esse documento estabelece as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no projeto e da propriedade intelectual de todos os produtos e conhecimento advindos da execução.

8.9.4. Além disso, o termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.

8.9.5. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços ao CONTRATANTE, bem como solicitar a revogação destas ao CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

8.9.6. Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

8.10. **Cyber Security Operations Center - CSOC**

8.10.1. Os serviços gerenciados de segurança devem ser executados por ambiente CSOC (Cyber Security Operation Center) próprio da CONTRATADA com sua infraestrutura de datacenter própria ou terceirizada em provedores especializados. A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto do presente termo de referência, o CSOC deve utilizar as infraestruturas de Data Centers e devem obrigatoriamente atender aos requisitos técnicos elencados, a saber:

8.10.1.1. Ambiente do Datacenter restrito, monitorado por Circuito Fechado de TV (CFTV), controlado e com registro de acesso físico, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Tais controles deverão estar disponíveis para pesquisa posterior pela Funpresp-Exe;

8.10.1.2. Rede elétrica estabilizada e com mais de uma entrada de alimentação;

8.10.1.3. Grupo gerador redundante e independente (N+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia comercial e autonomia mínima de 72 (setenta e duas) horas;

8.10.1.4. Sistema redundante de baterias para garantir a transição entre o fornecimento normal de energia e o grupo gerador;

8.10.1.5. Sistema de climatização redundante (N+1) para controle de temperatura do ambiente;

8.10.1.6. Ambiente do Datacenter com duas salas de interconexão de rede, independentes, entre o ambiente externo e a sala de equipamentos, e deve ser atendido por, pelo menos, duas empresas de telecomunicações, com rotas distintas entre si;

8.10.1.7. Piso suspenso com, no mínimo, 2 (duas) camadas de cabeamento, com vias independentes para cabos de energia, cabos UTP e cabos óticos;

8.10.1.8. Sistema de monitoração para controle de temperatura, umidade relativa do ar e filtros contra poeira;

8.10.1.9. Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo distribuídos pela área do Datacenter;

8.10.1.10. Sistema de detecção de fumaça, extintores manuais e brigada de incêndio;

8.10.1.11. O Centro de Dados onde os serviços estarão hospedados deverá ter disponibilidade de, no mínimo, 99,741%, sendo aceita a comprovação por meio de certificação TIA 942 TIER II;

8.10.1.12. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao CSOC;

8.10.1.13. Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

8.10.1.14. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

8.10.1.15. Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas desautorizadas;

8.10.2. A CONTRATADA deve comprovar que possui processos implementados que garantam a segurança das informações do CONTRATANTE, com base na norma ABNT NBR ISO/IEC 27001. Tal característica garante que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidente e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com o cliente.

8.11. **Inspeções e Diligências**

8.11.1. A contratação não será formalizada caso não haja o atendimento de quaisquer itens previstos no presente termo de referência.

8.11.2. A Funpresp-Exe reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las previamente à contratação.

8.11.3. A CONTRATANTE poderá realizar diligência no Cyber Security Operations Center - CSOC da CONTRATADA antes do início da prestação do serviço, in loco, a fim de validar e aferir se TODOS os itens solicitados no presente termo de referência serão atendidos.

8.11.4. Todos itens e serviços contratados pela Funpresp-Exe serão inclusos no ambiente tecnológico da Funpresp-Exe sendo a CONTRATADA responsável pela administração dos mesmos.

8.11.5. A CONTRATADA permitirá, a qualquer momento, a realização de diligências e vistorias em suas dependências, bem como prestar informações, com o intuito de avaliar os requisitos de Segurança da Informação, ficando a CONTRATADA responsável pelo atendimento das recomendações efetuadas.

8.11.6. A CONTRATADA permitirá, a qualquer momento, a realização de testes visando identificar falhas e vulnerabilidades no seu ambiente de TI, em suas dependências, bem como prestar informações, com o intuito de avaliar os requisitos de Segurança da Informação, ficando a CONTRATADA responsável pelo atendimento das recomendações efetuadas.

8.11.7. Caso a CONTRATADA possua rotina de verificação de vulnerabilidades do ambiente de TI, desde já se compromete a enviar relatórios destes testes, sempre que solicitado pelo CONTRATANTE, comprometendo-se a implementar as sugestões de melhorias que porventura forem produzidas.

8.12. **Plano de Continuidade de Negócios do CSOC**

8.12.1. A CONTRATADA deve apresentar o Plano de Continuidade de Negócios (PCN) da CONTRATADA, embasado em norma (ABNT NBR ISO 22301:2013 - Segurança da Sociedade - Sistema de Gestão de Continuidade de Negócios - Requisitos) ou boas práticas reconhecidas pelo mercado (ITIL v3, COBIT 5, Good Practice Guidelines - Business Continuity Institute, Professional Practices - Disaster Recovery Internacional Institute), para mitigar graves perdas decorrentes de riscos operacionais que possam comprometer o Acordo de Níveis de Serviço previstos neste CONTRATO.

8.12.2. O referido PCN e as evidências dos testes realizados devem ser entregues pela CONTRATADA para o CONTRATANTE, ao final da Etapa de Implantação do SISTEMA, quando da emissão do Termo de Aceitação Definitiva (TAD), anualmente e sempre que solicitado.

8.12.3. O Plano de Continuidade de Negócios apresentado pela CONTRATADA é analisado pelo CONTRATANTE que, motivadamente, pode rejeitar ou sugerir adequações de forma a atender aos Requisitos do Acordo de Níveis de Serviço.

8.12.4. Em caso de rejeição ou havendo necessidade de ajustes a CONTRATADA terá mais 30 (trinta) dias corridos, a partir da comunicação do CONTRATANTE, para retornar o plano atualizado.

8.12.5. Em caso de nova rejeição ou havendo necessidade de novos ajustes, a entrega do Plano de Continuidade de Negócios apresentado pela CONTRATADA terá um prazo estipulado para os ajustes necessários. Acordado ou revisto formalmente a qualquer tempo, o Projeto decorrente é classificado como uma Requisição, passando a ser considerado como integrante do Acordo de Níveis de Serviço, no Nível de Severidade e no prazo ajustado entre as PARTES, disto resultando a aplicação das respectivas Penalidades pelo não cumprimento.

8.13. **Segurança**

8.13.1. A CONTRATADA deverá observar quanto as questões de confidencialidade e responsabilidade dos produtos gerados a aderência às normas ABNT ISO/IEC NBR 27001:2013 e ABNT ISO/IEC NBR 27002:2013.

8.13.2. A CONTRATADA deverá possuir uma Política de Segurança da Informação e seus controles, entre eles, desde Segurança Física, Controle de Acesso, até a Gestão de Continuidade de Negócios.

8.14. **Sobre as Ferramentas a serem utilizadas**

8.14.1. Em todos os serviços desta contratação, as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

8.14.1.1. Deverá ser obrigatoriamente de propriedade ou licenciada para a CONTRATADA, possuir suporte do fabricante (quando aplicável) e não poderá ser do tipo open source (software livre).

8.14.1.2. Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.

8.14.1.3. Devem englobar a alocação de equipamentos e/ou softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;

8.14.1.4. Todos os equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso. Além disso, os equipamentos e softwares não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida;

8.14.1.5. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;

8.14.1.6. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

8.14.2. Em todas as especificações técnicas elencadas devem ser respeitadas as capacidades mínimas requeridas para os serviços entregues e que, no momento de contingência ou indisponibilidade de um equipamento ou software, os produtos alocados continuem suportando a operação sem degradação ou perda de performance.

8.15. **Da Instalação e Configuração de Equipamentos e Softwares**

8.15.1. A CONTRATADA deve ser responsável por prover todos os recursos necessários à instalação física de equipamentos, incluindo o fornecimento de cabos elétricos, cabos lógicos, adaptadores elétricos, parafusos, porcas, conectores, kits, racks, tomadas, transceivers/transceptores e demais materiais necessários à instalação de equipamentos nos locais de prestação dos serviços.

8.15.2. Os equipamentos e softwares necessários à prestação dos serviços devem estar cobertos por contratos de suporte técnico e garantia do fabricante durante o período de vigência de cada um dos itens de serviço.

8.15.3. Todos os elementos instalados devem ser configurados para envio de logs para a solução de consolidação e correlacionamento de eventos a ser implantada pela CONTRATADA. Este será o responsável pela coleta, processamento, normalização, armazenamento e correlação de eventos gerados pelos diversos servidores de rede e de aplicação. Dessa forma, as atividades de levantamento, desenvolvimento de conectores e implantação de casos de uso de correlacionamento da solução implantada deve fazer parte das etapas de implantação da solução.

8.15.4. Faz parte da fase de instalação a interação com as equipes da CONTRATANTE para configuração das rotinas de backup da solução ofertada e da realização de testes de restore e de desligamento/religamento da solução.

8.15.5. Finalmente, todas as configurações existentes na solução de segurança atualmente instalada na CONTRATANTE devem ser avaliadas e os elementos a serem instalados devem ser configurados de forma a compatibilizar as regras àquelas existentes na CONTRATANTE, com os ajustes necessários para melhoria e otimização, de forma a garantir nível de segurança igual ou superior.

8.16. **Documentação**

8.16.1. Após a ativação dos serviços e migração tecnológica, deve ser entregue a CONTRATANTE documentação de as-built de cada serviço, contendo as seguintes informações:

a) Descrição dos serviços implantados.

b) Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços.

c) Dados dos equipamentos e softwares, incluindo configurações, números de série e versões.

d) Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares.

e) Definição de responsabilidades.

f) Recursos de alta disponibilidade.

g) Scripts de operação, incluindo desligamento e ligamento, switch over, acionamento do equipamento de contingência, quando necessário.

h) Procedimentos para abertura e atendimento a chamados.

i) Procedimentos de recuperação de equipamentos.

j) Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas.

k) Rotinas periódicas configuradas.

l) Documentação dos processos de trabalho associados ao item, em esquema de fluxograma, com definição de responsáveis por cada atividade, prazos de execução, rotinas de atualização e revisão periódica de regras.

m) Casos de uso implantados na solução de correlacionamento.

n) Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos)

8.16.2. A entrega pela CONTRATADA da documentação as-built e aprovação pela CONTRATANTE é condição necessária para emissão do termo de recebimento definitivo de cada item de serviço, conforme condições expostas na cláusula que trata do recebimento do objeto.

8.17. **Da Transição Contratual**

8.17.1. Ao final do contrato, a CONTRATADA deve elaborar e entregar documentação técnica de transição contratual para cada um dos Serviços Gerenciados de Segurança, como subsídio para contratações futuras. Tais documentos são responsáveis por assegurar a confidencialidade, integridade e disponibilidade dos serviços de TI no momento de migrações futuras da solução implementada, incluindo as seguintes informações:

8.17.1.1. Documentação técnica atualizada de as-built da solução, incluindo parâmetros de instalação e configuração.

8.17.1.2. Demonstrativo de crescimento anual de capacidade da solução implementada.

8.17.1.3. Baseline de dados que subsidiem a planejamento de capacidade dos serviços, incluindo informações estatísticas de uso de recursos de hardware e software.

8.17.1.4. Fornecimento de arquivos de configuração dos produtos.

9. **DEVERES E RESPONSABILIDADES**

9.1. **Deveres e responsabilidades da CONTRATANTE:**

9.1.1. Acompanhar e fiscalizar a execução do contrato;

9.1.2. Alocar os recursos necessários à execução dos serviços ora contratados;

9.1.3. Fornecer à CONTRATADA todas as informações que esta necessitar para poder cumprir adequadamente o presente contrato;

9.1.4. Rejeitar, no todo ou em parte, os serviços fora do estabelecido e que estejam em desacordo com os requisitos obrigatórios do Termo de Referência, seus ANEXOS e Contrato;

9.1.5. Efetuar o pagamento da nota fiscal/fatura apresentada pela CONTRATADA, conforme o prazo e as condições estabelecidos no presente instrumento;

9.1.6. Notificar a CONTRATADA de qualquer irregularidade verificada na execução das atividades;

9.1.7. Não utilizar os funcionários da CONTRATADA para execução de outros serviços que não aqueles aqui contratados, da mesma forma, não poderá pagar compensações ou fornecer qualquer outro benefício aos funcionários da CONTRATADA;

9.1.8. Permitir ao pessoal da CONTRATADA acesso ao local da entrega desde que observadas as normas de segurança.

9.1.9. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência;

9.1.10. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

9.1.11. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

9.1.12. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

9.1.13. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

9.1.14. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Fundação, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

9.1.15. Outras obrigações que se apliquem, de acordo com o objeto da contratação.

9.2. **Deveres e responsabilidades da CONTRATADA:**

9.2.1. Cumprir o disposto no inciso XXXIII do art. 7º da Constituição Federal, que proíbe trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos;

9.2.2. Cumprir as legislações e regulamentações relativas à prevenção e ao combate à corrupção, lavagem de dinheiro, financiamento do terrorismo e fraude;

9.2.3. Responsabilizar-se por todas as obrigações trabalhistas e previdenciárias, FGTS, seguro e quaisquer encargos propostos, não existindo entre seus empregados e o CONTRATANTE vínculo de qualquer natureza, haja vista que a CONTRATADA, para todos os fins de direito, é empregadora autônoma;

9.2.4. Cumprir e manter, durante toda a vigência contratual, padrões elevados de ética, respeitando: a legislação brasileira e os compromissos internacionais assumidos pelo Estado Brasileiro que tratam de direitos humanos e/ou da responsabilidade socioambiental; os padrões ambientais legalmente estabelecidos; e as exigências legais acerca das responsabilidades trabalhistas e da proibição do trabalho escravo e do trabalho infantil;

9.2.5. Manter o mais completo e absoluto sigilo, para os jurídicos e legais efeitos, devendo guardar, por si, seus empregados e/ou prepostos, em relação às informações, documentos de qualquer natureza e tecnologia que, em razão deste instrumento, lhe sejam exibidos, manuseados ou por qualquer outra forma ou modo, venham a tomar conhecimento, ficando, portanto, responsáveis por sua indevida divulgação, descuidada ou incorreta utilização, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;

9.2.6. Pagar todos os tributos, contribuições fiscais e parafiscais que incidam direta ou indiretamente sobre este contrato ou seu objeto, ficando, desde logo, convencionado que o CONTRATANTE poderá descontar de qualquer crédito da CONTRATADA a importância correspondente a eventuais pagamentos desta natureza, que porventura venha a efetuar por imposição legal, podendo também o CONTRATANTE exigir, se e quando necessário, a apresentação dos respectivos comprovantes de quitação dos períodos anteriores;

9.2.7. Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE, cujas reclamações se obriga atender prontamente;

9.2.8. Responder por todo e qualquer dano que causar diretamente ao CONTRATANTE ou a terceiros, ainda que culposo, praticado comprovadamente por seus prepostos, empregados ou mandatários, não excluindo ou reduzindo essa responsabilidade à fiscalização ou acompanhamento pelo CONTRATANTE;

9.2.9. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas por lei e neste instrumento, inclusive a regularidade fiscal;

9.2.10. Registrar as ocorrências havidas durante a execução do contrato, de tudo dando ciência ao CONTRATANTE, respondendo integralmente por sua omissão;

9.2.11. Dar ciência ao CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços, mesmo que estes não sejam de sua competência;

9.2.12. Observar os critérios de sustentabilidade ambiental, tendo por fundamento, a Constituição Federal, a lei nº 13.303/16, compromissos internacionais assumidos pelo Estado Brasileiro, e outras legislações pertinentes, particularmente a lei Federal nº 12.187, de 29 de dezembro de 2009, que instituiu a Política Nacional sobre Mudança do Clima e a Lei Federal nº 12.305, de 02 de agosto de 2010, que instituiu a Política Nacional de Resíduos Sólidos;

9.2.13. Cumprir, no que couber, as exigências do inciso XI, art. 7° da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS;

9.2.14. Observância aos normativos internos da Funpresp-Exe, dentre os quais se encontra sua Política de Responsabilidade Socioambiental;

9.2.15. Indicar formalmente e por escrito um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

9.2.16. Fornecer o objeto deste contrato pelos preços contratados e de acordo com o previsto nas especificações deste termo bem como dos seus anexos, sem nenhum ônus extra para o CONTRATANTE;

9.2.17. Responsabilizar-se civilmente por vícios no fornecimento tais como: quantidade, qualidade do produto ou disparidade com as especificações técnicas exigidas neste termo, ou atribuídas pela CONTRATADA, verificados posteriormente, garantindo-se ao CONTRATANTE as faculdades previstas no art. 18 da Lei n.º 8.078/90, do Código de Defesa do Consumidor.

9.2.18. Prestar os serviços definidos no objeto, nas especificações e nas condições deste instrumento, com pessoal adequadamente capacitado, utilizando todos equipamentos/padrões de segurança associados;

9.2.19. Fiscalizar o perfeito cumprimento dos serviços a que se obrigou, cabendo-lhe, integralmente, os ônus decorrentes. Tal fiscalização dar-se-á independente da que será exercida pelo CONTRATANTE;

9.2.20. Não permitir que seus empregados ou prepostos executem serviços além dos previstos no objeto deste contrato;

9.2.21. Efetuar os serviços através de pessoas idôneas, e devidamente identificadas por crachá, assumindo total responsabilidade por quaisquer danos ou faltas que os mesmos venham a cometer no desempenho de suas funções, podendo o CONTRATANTE exigir a retirada daqueles cuja conduta seja inconveniente, obrigando-se, também, a indenizar o CONTRATANTE por todos os danos e prejuízos que eventualmente ocasionar, após ficar comprovado que os mesmos foram causados pela CONTRATADA, através de seus prepostos, empregados ou mandatários, ficando o CONTRATANTE autorizado a descontar o valor correspondente dos pagamentos à CONTRATADA. Caso os serviços venham a ser executados nas dependências do CONTRATANTE, os profissionais da CONTRATADA ficarão submetidos às normas internas de segurança.

9.2.22. Responsabilizar-se pela integral prestação de serviços, inclusive no que se referir a inobservância da legislação em vigor.

9.2.23. A CONTRATADA obriga-se a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço.

9.2.24. A notificação deve ocorrer também na situação em que a interrupção for motivada por inadimplência do CONTRATANTE.

9.2.25. A Contratada deverá observar rigorosamente todas as condições previstas neste Termo de referência, Contrato e seus anexos, inclusive, comunicar ao Contratante, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos necessários.

9.2.26. A CONTRATADA deve realizar a integração com os sistemas de gerenciamento de identidades – IDM da Funpresp-Exe.

9.2.27. Documentos/Procedimentos que garantam a CONTRATANTE o acesso sob demanda aos relatórios elaborados por empresas de auditoria para a CONTRATADA;

9.2.28. As senhas das contas com permissão administrativa devem ser armazenadas exclusivamente no repositório da solução de gestão de usuários da Funpresp-Exe.

9.2.29. As implantações e integrações devem ocorrer primeiramente em ambiente de homologação, separados do ambiente de produção, para avaliação dos gestores. Somente após a liberação dos gestores poderão ser implantados em ambiente de produção.

9.2.30. Em infraestrutura de nuvem, a CONTRATADA deve prover mecanismos para assegurar a confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas e armazenadas.

9.2.31. Em infraestrutura de nuvem, a CONTRATADA deve prover mecanismos para auditoria pela Funpresp-Exe, dos serviços prestados em conformidade com sua regulamentação.

9.2.32. Em infraestrutura de nuvem, a CONTRATADA deve prover o acesso da Funpresp-Exe aos instrumentos de monitoramento e gestão dos controles adotados para a solução contratada.

9.2.33. A CONTRATADA deve comunicar tempestivamente a CONTRATANTE sobre incidentes relevantes e interrupções dos serviços prestados que venham ocorrer e configurem uma situação de crise;

9.2.34. A CONTRATADA deve emitir relatório de vulnerabilidades previamente a liberação de novas versões das aplicações, caso o serviço contratado entregue software como serviço (SaaS), que poderá ser solicitado pela CONTRATANTE durante a vigência contratual.

9.2.35. Participar, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais (reunião inicial) com uma equipe técnica da Funpresp. A Funpresp-Exe fará a convocação dos representantes da empresa e fornecerá previamente a pauta da reunião.

9.2.36. No momento da assinatura do contrato, indicar, formalmente, preposto e substituto eventual que tenha capacidade gerencial e de coordenação para tratar de todos os assuntos previstos neste Termo de Referência e no instrumento contratual correspondente, sem implicar em ônus para o Contratante, quando do exercício dessa função. Assim como fornecer os telefones de contato dos indicados.

9.2.37. Encaminhar à Funpresp-Exe, sempre que houver afastamentos legais ou substituição de funcionários, relação nominal dos profissionais que atuarão junto à Fundação, indicando CPF, área de atuação, curriculum vitae e comprovação de certificações e experiência.

9.2.38. Providenciar e manter a qualificação técnica adequada dos profissionais que prestam serviços para a fundação, de acordo com as necessidades pertinentes à adequada execução dos serviços contratados durante todo o período de contratação.

9.2.39. Assinar o termo de confidencialidade constante do Anexo 14 deste Termo de Referência e parte integrante deste, quando da assinatura do instrumento contratual.

9.2.40. Será exigido que a empresa demonstre que está em conformidade com a LGPD, sendo essa demonstração analisada pela área de Proteção de Dados da Funpresp-Exe;

9.2.41. Os requisitos impostos pela LGPD podem ser observados por meio de políticas de privacidade e proteção de dados, medidas e boas práticas implementadas na empresa – preferencialmente com a apresentação de Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto no inciso XVII do art. 5º da referida Lei;

9.2.42. A empresa deverá possuir/apresentar:

a) Encarregado de proteção de dados nomeado com as informações do responsável publicadas no website;

b) Políticas de Privacidade e Proteção de Dados;

c) Medidas e boas práticas implementadas na empresa para conformidade à LGPD;

d) Relatório de Impacto à Proteção de Dados Pessoais - RIPD.

9.2.43. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

9.2.44. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

9.2.45. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

9.2.46. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

9.2.47. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

9.2.48. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Fundação;

9.2.49. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

9.2.50. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;

9.2.51. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

10. MODELO DE EXECUÇÃO DO CONTRATO

10.1. Rotinas de Execução

10.1.1. Devido à complexidade e à criticidade dos serviços gerenciados de segurança objeto desta contratação, a execução do contrato será dividida em três etapas: Implantação do Serviço; Operação do Serviço; Encerramento/Transição do Serviço.

10.1.1.1. 1ª fase: Implantação do Serviço

a) Reunião inicial para apresentação do preposto da CONTRATADA, a ser convocada pela Funpresp-Exe em até 10 (dez) dias úteis após assinatura do contrato;

b) Serviços e aspectos de infraestrutura para a implantação dos serviços;

c) Definição do canal de atendimento para o reporte de incidentes, problemas e solicitações de serviços;

d) Definição de papéis e responsabilidades e cronograma físico de ativação dos equipamentos e ambientes para a Funpresp-Exe (CONTRATADA);

10.1.1.2. 2ª fase: Operação do Serviço

a) Para aferição da prestação de serviços, a CONTRATADA do serviço gerenciado de segurança deverá enviar relatórios mensais, conforme apresentado no item 6.3.1, até o 10º dia útil do mês subsequente;

b) Para efeito de fiscalização, as informações apresentadas serão comparadas com mecanismos de controle independentes, de responsabilidade da Funpresp-Exe;

c) Em conjunto com estes relatórios, a CONTRATADA deverá apresentar prévia de faturamento, a ser analisada pela equipe de fiscalização;

d) A entrega da totalidade dos documentos dos itens A e B acima ensejará a emissão do Termo de Recebimento Provisório;

e) O parecer sobre os documentos apresentados, os ajustes na prévia de faturamento, bem como a aplicação de glosas na execução do serviço, serão encaminhadas à CONTRATADA do serviço em até 5 dias úteis contados do recebimento;

f) A CONTRATADA do serviço poderá emitir considerações sobre o parecer da equipe de fiscalização, que serão avaliadas por esta em até 5 dias úteis, quando haverá a emissão do Termo de Recebimento Definitivo;

g) Após esta última etapa de avaliação, a CONTRATADA do serviço será autorizada a emitir as Notas Fiscais para pagamento;

10.1.1.3. **3ª fase: Encerramento/Transição do Serviço**

a) A CONTRATADA deverá envidar esforços para a correta e tempestiva transferência de informações/conhecimentos e dados para o sucessor na prestação dos serviços, inclusive mediante participação efetiva das equipes técnicas no planejamento.

10.2. **Prazos e Formas de Entrega para Fornecimento de Bens / Prestação de Serviços**

10.2.1. O cronograma previsto para os eventos da gestão contratual é o que segue:

Serviço Gerenciado de Segurança		
Evento	**Prazo**	**Contagem**
Assinatura do Contrato	D	N/A
Recebimento da cópia assinada do contrato	D+0	N/A
Prestação da garantia (5% do valor total anual)	D+10	dias úteis
Início da etapa de implantação do serviço	D+1	N/A
Apresentação do Plano de Implantação pela Contratada	T = D+10	dias corridos
Aprovação do Plano de Implantação pela Funpresp-Exe	T + 5	dias corridos
Reunião de iniciação do contrato entre Contratada e Funpresp-Exe	Até D+10	dias corridos
Início da execução contratual pela Contratada	Até D+60	dias corridos
Uso da garantia, pela Funpresp-Exe, para cumprimento de obrigações da Contratada	Final da vigência + 90 dias	N/A
Uso da garantia total ou parcialmente pela Funpresp-Exe	Ocorrência + 48 horas	N/A
Renovação, utilização ou recálculo da garantia prestada pela Contratada	Data de ocorrência + 10	dias úteis
Restituição da garantia pela Funpresp-Exe	Final da vigência do contrato + 90 dias	N/A
Elaboração do relatório de execução de atividades especializadas	Até o 10º (décimo) dia útil do mês subsequente à prestação dos serviços	N/A
Recolhimento de multa por atraso injustificado na execução do objeto do Contrato, ou o descumprimento das obrigações	Data de Notificação + 15	dias úteis
Recolhimento de multa pela inexecução total ou parcial	Data de notificação + 15	dias úteis
Encaminhamento da previa da fatura pela Contratada	Até o 10º (décimo) dia útil do mês subsequente à prestação dos serviços	dias úteis
Avaliação e parecer dos relatórios e da prévia da fatura para pagamento pela equipe de fiscalização	Data de recebimento da prévia + 2	dias úteis
Autorização de emissão da Nota Fiscal / Fatura pela Contratada	Data de emissão do parecer da equipe de fiscalização + 2	Dias úteis
Encaminhamento da Nota Fiscal / Fatura pela Contratada para atesto pelo Gestor do Contrato	Até o 3º (terceiro) dia útil da autorização de emissão da Nota Fiscal / Fatura	Dias úteis
Realização do pagamento pela Funpresp-Exe	Data do recebimento da NF + 15	dias úteis
Regularização da situação de inadimplência da Contratada	Data da Notificação da Funpresp-Exe + 30	dias corridos

10.3. **Documentação Mínima Exigida**

10.3.1. A CONTRATADA deverá disponibilizar, mensalmente, relatórios gerenciais que demonstrem a execução das atividades para que a Funpresp-Exe possa atestar o provimento dos serviços. Minimamente, a CONTRATADA deverá apresentar, eletronicamente, as seguintes informações:

10.3.1.1. Lista de ações executadas nos serviços de Gestão de Vulnerabilidades;

10.3.1.2. Lista dos ataques cibernéticos aplicáveis ao ambiente da Funpresp-Exe para o planejamento e execução de ações de melhoria nos serviços tecnológicos;

10.3.1.3. Listagem de incidentes de segurança reportados no período, além dos incidentes sem causa-raiz identificada e mitigada;

10.3.1.4. Listagem de chamados referentes às requisições e atividades nas ferramentas de antivírus, firewall e recursos de rede, além das políticas criadas para atendimento dessas requisições;

10.3.1.5. Plano de atividades de conscientização a serem executadas junto aos usuários, além dos resultados atingidos pelas campanhas realizadas;

10.3.1.6. Serviços técnicos especializados executados, de acordo com o acordado com a equipe técnica da Funpresp-Exe.

10.3.2. As informações fornecidas pela(s) CONTRATADA(s) serão confrontadas, quando aplicável, a controles mantidos pela equipe técnica da Funpresp-Exe, para a aferição e comprovação dos serviços prestados.

10.4. **Papéis e Responsabilidades**

10.4.1. Fiscal do Contrato, com as seguintes atribuições:

10.4.1.1. Elaboração do Plano de Inserção da CONTRATADA;

10.4.1.2. Convocação e realização de reunião inicial;

10.4.1.3. Encaminhamento formal de Ordem de Serviço;

10.4.1.4. Encaminhamento das demandas de correção à CONTRATADA, quando houver;

10.4.1.5. Encaminhamento de indicação de sanções à GELOG, quando as houver;

10.4.1.6. Analisar desvios de qualidade;

10.4.1.7. Elaborar termo de recebimento definitivo do serviço de migração;

10.4.1.8. Autorizar à CONTRATADA a emissão de Notas Fiscais;

10.4.1.9. Encaminhamento de pedidos de alteração contratual à GELOG, quando os houver;

10.4.1.10. Manutenção do Histórico de Gerenciamento do Contrato;

10.4.1.11. Encaminhar justificativa para aditamento contratual à GELOG se julgado conveniente e oportuno.

10.4.2. Representante da CONTRATADA, com as seguintes atribuições:

10.4.2.1. Participar da reunião inicial, apresentando o preposto, entregando o termo de compromisso e o termo de ciência assinados e prestando e recebendo esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.

10.4.3. Preposto da CONTRATADA, com as seguintes atribuições:

10.4.4. Participar da reunião inicial;

10.4.5. Receber Ordens de Serviço;

10.4.6. Receber autorização para emissão de Notas Fiscais;

10.4.7. Entregar termo de ciência assinado pelos novos empregados em casos de inclusão/substituição;

10.4.8. Garantir a aderência dos serviços prestados aos termos da contratação;

10.5. **Mecanismos formais de comunicação**

10.5.1. A(s) CONTRATADA(s) deverá(ão) disponibilizar canais de contato para a abertura de chamados e consultas técnicas, reporte de incidentes e abertura de solicitações para todos os serviços contratados, via web, telefone e e-mail, durante 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;

10.5.2. Além disso, para fins de controle e auditoria, a(s) CONTRATADA(s) deve(m) disponibilizar acesso às fontes das informações supracitadas para a equipe técnica da Funpresp-Exe, a qualquer tempo, através de sistema informatizado;

10.5.3. Quaisquer questões administrativas durante a execução do contrato, de cunho mais formal, deverão encaminhadas entre as partes por envio de Ofício via correio eletrônico, com confirmação de recebimento;

10.5.4. Questões administrativas cotidianas durante a execução do contrato poderão ser encaminhadas através de mensagem eletrônica (e-mail) entre as partes.

10.6. **Manutenção de Sigilo e Normas de Segurança**

10.6.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

10.6.2. O **Termo de Compromisso e Manutenção de Sigilo**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos anexos 14 e 15 do termo de referência.

11. **MODELO DE GESTÃO DO CONTRATO**

11.1. **Critérios de Aceitação**

11.1.1. O acompanhamento e a fiscalização da execução do contrato consistem-se na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato.

11.1.2. O fiscal do contrato deverá monitorar constantemente o nível de qualidade dos serviços para evitar prejuízos, devendo intervir para corrigir ou aplicar sanções quando verificar um viés contínuo de desconformidade da prestação do serviço à qualidade exigida, no tocante às suas atribuições.

11.1.3. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

11.1.4. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste documento.

11.1.5. O responsável pelo acompanhamento e fiscalização deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato, cuja incumbência é monitorar constantemente o nível de qualidade dos serviços para evitar prejuízos, devendo intervir

para corrigir ou aplicar sanções quando verificar um viés contínuo de desconformidade da prestação do serviço à qualidade exigida, no tocante às suas atribuições, podendo, inclusive, culminar em rescisão contratual.

11.1.6. A execução do contrato deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos seguintes aspectos:

a) Os resultados alcançados em relação aos serviços, com a verificação dos prazos de execução e da qualidade demandada.

b) Os recursos humanos empregados, em função da quantidade e disponibilidade exigidas.

c) A adequação dos serviços prestados à rotina de execução estabelecida.

d) Verificar o cumprimento das demais obrigações decorrentes do contrato.

e) Consultar a regularidade fiscal da CONTRATADA.

11.1.7. A fiscalização não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros por qualquer irregularidade, ou ainda, resultante de imperfeições técnicas ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE.

11.1.8. À CONTRATANTE será reservado o direito de rejeitar no todo ou em parte os serviços prestados, se em desacordo com o Edital, devendo a CONTRATADA refazer os serviços rejeitados sem ônus adicionais, no prazo fixado pelo fiscal do contrato.

11.1.9. O representante da CONTRATANTE deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

11.1.10. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual.

11.1.11. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha a respectiva relação detalhada, de acordo com o estabelecido neste documento e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

11.2. **Procedimentos de Teste e Inspeção**

11.2.1. A ADJUDICATÁRIA deverá preencher e apresentar o Anexo 17 – Verificação de Soluções antes da homologação do certame e sempre que houver modificação nos equipamentos e softwares fornecidos para compor a solução de TI;

11.3. **Níveis Mínimos de Serviço**

11.3.1. Os níveis mínimos de serviço encontram-se no anexo 10 do Termo de Referência.

11.4. **Das Infrações e das Sanções Administrativas**

11.4.1. A aplicação de penalidades e sanções administrativas observará o disposto no Regulamento Interno de Licitações e Contratos da Funpresp-Exe e na Lei nº 13.303/2016.

11.4.2. A licitante que praticar ou que tenha praticado atos ilícitos visando frustrar os objetivos desta licitação, poderá ser aplicada a sanção de suspensão temporária de participação em licitação e impedimento de contratar com a Funpresp-Exe, por até 2 (dois) anos.

11.4.3. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

11.4.4. A licitante/Adjudicatária que cometer qualquer das infrações discriminadas nos itens 12.6, 12.7 e 12.8 , ficará sujeita, sem prejuízo da responsabilidade civil e criminal, ao impedimento de licitar e de contratar com a Funpresp-Exe e descredenciamento no SICAF, pelo prazo de até 02 (dois) anos.

11.4.5. Além das penalidades previstas nos itens antecedentes, a inexecução total ou parcial do objeto contratado sujeitará a CONTRATADA, garantida a prévia defesa, às seguintes sanções, observado o procedimento para aplicação de sanções previsto no Regulamento de Licitações e Contratos da Funpresp-Exe:

I - Advertência;

II - Multa, aplicável nos percentuais e casos adiante enumerados:

a) No caso de inexecução parcial do objeto, multa na razão de 3% (três por cento) sobre o valor total atualizado do objeto contratado;

b) No caso de inexecução total, multa na razão de 5% (cinco por cento), sobre o valor total atualizado do objeto contratado.

III - Suspensão temporária de participação em licitação e impedimento de contratar com o CONTRATANTE, por prazo não superior a 2 (dois) anos.

11.4.6. Além das condutas irregulares previstas na Lei nº 12.846/2013, a sanção de suspensão estabelecida no inciso III do item 12.4.6, poderá também ser aplicada à CONTRATADA se esta:

I - Sofrer condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II - Demonstrar não possuir idoneidade para contratar com o CONTRATANTE em virtude de atos ilícitos praticados.

11.4.7. As multas previstas no inciso II do item 12.4.6 quando aplicadas, serão descontadas dos pagamentos eventualmente devidos pelo CONTRATANTE à CONTRATADA ou, ainda, quando for o caso, cobradas administrativa ou judicialmente.

11.4.8. O atraso injustificado na execução do objeto contratado sujeitará a CONTRATADA à multa de mora, de 0,1% (um décimo por cento) por dia sobre o valor total contratado.

11.4.9. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa.

11.4.10. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Funpresp-Exe, observado o princípio da proporcionalidade.

11.4.11. As multas serão recolhidas em favor do CONTRATANTE, no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente, ou, quando for o caso, cobradas judicialmente.

11.4.12. As sanções previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.

11.4.13. Sem prejuízo da aplicação das sanções acima descritas, a prática de quaisquer atos lesivos à Funpresp-Exe na licitação ou na execução do objeto, nos termos do Regulamento Interno de Licitações e Contratações da Funpresp-Exe, será objeto de imediata apuração observando-se o devido processo legal estabelecido.

11.5. **Do Pagamento**

11.5.1. Os serviços serão pagos com periodicidade mensal.

11.5.2. O pagamento será efetuado em até 15 (quinze) dias após após o ateste, pelo fiscal do contrato, da nota fiscal/fatura, devendo para isto, ficar explicitado o nome do banco, agência, localidade e número da conta-corrente em que deverá ser efetivado o crédito.

11.5.3. Havendo erro na Nota Fiscal ou circunstância que impeça a liquidação da despesa, aquela será devolvida à Contratada e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a Contratante.

11.5.4. Antes de cada pagamento será verificada a regularidade fiscal da contratada perante o INSS e o FGTS.

11.5.5. Constatando-se a situação de irregularidade da contratada perante o INSS e o FGTS será providenciada sua notificação, por escrito, para que, apresente defesa.

11.5.6. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação fiscal.

11.5.7. Poderá ser rescindido o contrato em execução com a contratada inadimplente, salvo por motivo de economicidade ou outro de interesse da Funpresp-Exe de alta relevância, devidamente justificado e, em qualquer caso, aprovado pela Diretoria Executiva da Funpresp-Exe.

11.5.8. Dos pagamentos devidos à Contratada serão retidos os impostos e contribuições de acordo com a legislação vigente, em especial a prevista no art. 31 da Lei 8.212/1993.

11.5.9. A empresa a ser contratada deverá informar, quando da assinatura do instrumento contratual, o enquadramento tributário a ser dado ao objeto da contratação, para fins de avaliação de sua pertinência pela Funpresp-Exe.

11.5.10. Caso o contratado seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, junto à Nota Fiscal/Fatura, a devida declaração, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

11.5.11. As eventuais multas impostas ao Contratado em decorrência de inadimplência contratual poderão ser descontadas do pagamento devido desde que concluído o procedimento para aplicação de sanções.

11.5.12. À Contratante reserva-se o direito de recusar o pagamento se no ato da atestação os serviços realizados não estiverem em perfeitas condições ou em desacordo com as especificações apresentadas e aceitas.

11.5.13. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Funpresp-Exe, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

EM = I x N x VP, onde:

EM = Encargos Moratórios devidos;

I= Índice de compensação financeira = 0,00016438, computado com base na fórmula I = [(TX/100)/365];

N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; e

VP = Valor da prestação em atraso.

12. **VALOR ESTIMADO DA CONTRATAÇÃO**

12.1. O valor estimado para esta contratação está descrito abaixo. Não serão aceitas propostas acima deste valor.

CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - 36 MESES			
Total Grupo 01 (36 meses) (A)	Total Grupo 02 (1440 horas) (B)	Total Grupo 03 (36 meses) (C)	Valor Global Estimado (36 meses) (D = A + B + C)
R$ 13.743.743,40	**R$ 678.268,80**	**R$ 1.366.200,00**	**R$ 15.788.212,20**

13. **ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO**

13.1. O investimento está previsto no PDTI 2022-2023 e as despesas decorrentes da contratação correrão às expensas dos recursos constantes do Plano de Gestão Administrativa - PGA da FUNPRESP-EXE, do ano de 2023.

14. **DA VIGÊNCIA DO CONTRATO**

14.1. O contrato a ser firmado terá vigência de 36 meses podendo ser prorrogado até o limite de 60 (sessenta) meses.

14.2. A vigência justifica-se com vistas a permitir que o período contratual acomode contínuos processos de planejamento, implantação, configuração, migração, estabilização, revisão e disponibilização dos serviços de Segurança da Informação continuados.

15. **DO REAJUSTE DE PREÇOS**

15.1. Por se tratar de contratação de Serviços de Tecnologia da Informação é obrigatória a adoção do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA.

15.2. Será concedido reajuste dos preços dos serviços continuados com prazo de vigência igual ou superior a 12 (doze) meses desde que observado o interregno mínimo de 01 (um) ano, contado da data limite para a apresentação da proposta.

15.3. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação então em vigor.

15.4. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente.

15.5. Não está previsto o instrumento de "repactuação" para o presente CONTRATO, uma vez que o presente CONTRATO é puramente de prestação de serviços. O reajuste será realizado por apostilamento.

16. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1. Regime, Tipo e Modalidade da Licitação

16.1.1. A contratação se dará por meio de Pregão Eletrônico por menor preço.

16.2. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

16.2.1. Não se vislumbra a aplicabilidade da margem de preferência ao objeto em tela.

16.3. Critérios de Qualificação Técnica para a Habilitação

16.3.1. As empresas participantes do processo deverão apresentar as seguintes comprovações quanto ao objeto licitado:

16.3.1.1. Comprovação de aptidão para execução das atividades pertinentes e compatíveis com os serviços, através da apresentação de 01 (um) ou mais atestados, fornecidos por empresas de direito público ou privado, devendo observar o que segue:

a) Os atestados deverão comprovar, de forma explícita, que a licitante executou os serviços, com características e prazo, pertinentes e compatíveis com o objeto deste edital;

b) Serão aceitos atestados expedidos durante e após a conclusão do contrato, sendo considerado o prazo decorrido entre o início do contrato e a emissão do atestado;

c) Será aceita a somatória de atestados para comprovação da qualificação técnica desde que a soma dos itens atenda as quantidades mínimas exigidas.

d) Os atestados deverão ser apresentados em papel timbrado do emitente e conter a identificação do signatário, nome, endereço completo, telefone e correio eletrônico corporativo para contato;

e) A licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foram prestados os serviços e notas fiscais;

f) O atestado poderá ser emitido para empresa do mesmo grupo econômico, desde que a mesma seja a prestadora final do serviço contratado neste processo licitatório.

16.3.1.2. Documento(s) que comprove(m) a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, para o contrato de no mínimo 12 meses em ambiente compatível com o do CONTRATANTE.

16.3.1.3. Para o Grupo 1:

a) experiência na prestação de serviços de operação e resposta a requisições, incluindo a administração de solução de antivírus, EDR ou antimalware para estações de trabalho em ambiente computacional com, no mínimo, 400 (quatrocentos) endpoints;

b) experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas em ambientes com, no mínimo, 200 (duzentos) ativos;

c) experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação - SIEM, em ambientes com, no mínimo, 1.250 (mil duzentos e cinquenta) eventos por segundo (EPS);

d) experiência na prestação de serviços de resposta a incidentes de segurança, incluindo a criação de um Plano de Resposta a Incidentes e de Assessment & Mitre Attack;

e) experiência na prestação de serviços de proteção de tráfego de borda, incluindo a administração de solução de Firewall, UTM ou NGFW;

f) experiência na prestação de serviços de implantação, instalação ou administração de solução de WAF;

g) experiência na prestação de serviços de inteligência aplicada à segurança, por meio da prestação de serviços, administração e operação de solução de inteligência para no mínimo, 7 (sete) alvos/ativos monitorados;

h) experiência na prestação de serviços de conscientização, por meio da prestação de serviços para no mínimo, 250 usuários.

16.3.1.4. Para o Grupo 2:

a) experiência na prestação de serviços de serviço técnico especializado similar ao objeto especificado com no mínimo 500 horas.

16.3.1.5. Para o Grupo 3:

a) experiência na prestação de serviço de teste de invasão (PENTEST) para exploração de vulnerabilidades de segurança da informação;

16.3.2. O CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando validar ou esclarecer informações sobre o serviço prestado.

17. CRITÉRIOS TÉCNICOS PARA JULGAMENTO DA PROPOSTA

17.1. O licitante provisoriamente classificado em primeiro lugar deverá apresentar juntamente com a proposta comercial, as referências de cada item da especificação de cada equipamento ou serviço com os manuais técnicos de descrição do fabricante, elencando a página que se encontra

a referida especificação. Todas as especificações requeridas devem possuir as devidas referências dos componentes de hardware e de software componentes da solução ofertada, com vistas à avaliação de aderência destes aos requisitos constantes nos Anexos.

18. **DA PARTICIPAÇÃO EM CONSÓRCIO**

18.1. Para a prestação destes serviços não serão admitidas a formação de consórcios ou a contratação de cooperativas.

19. **DA SUBCONTRATAÇÃO**

19.1. Para a prestação destes serviços não serão admitidas subcontratações.

20. **DA ALTERAÇÃO SUBJETIVA**

21. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Funpresp-Exe à continuidade do contrato.

22. **DAS DISPOSIÇÕES FINAIS**

22.1. Integram este Termo de Referência os seguintes Documentos:

a) Matriz de Riscos (SEI nº 0128405);
b) Anexo 1 - Serviço de Operação e Resposta a Requisições (SEI nº 0127345);
c) Anexo 2 - Serviço de Gestão de Vulnerabilidades (SEI nº 0127349);
d) Anexo 3 - Serviço de Monitoramento de Ataques Cibernéticos (SEI nº 0127422);
e) Anexo 4 - Serviço de Resposta a Incidentes de Segurança (SEI nº 0127423);
f) Anexo 5 - Serviço de Proteção de Tráfego de Borda (SEI nº 0127424);
g) Anexo 6 - Serviço de Inteligência Aplicada à Segurança (SEI nº 0127430);
h) Anexo 7 - Serviço de Conscientização de Segurança da Informação (SEI nº 0127431);
i) Anexo 8 - Serviços Técnicos Especializados (SEI nº 0127436);
j) Anexo 9 - Serviço de Teste de Invasão (SEI nº 0127437);
k) Anexo 10 - Níveis Mínimos de Serviços (SEI nº 0127439);
l) Anexo 11 - Catálogo de Serviços (SEI nº 0127440);
m) Anexo 12 - Ambiente Funpresp (SEI nº 0127442);
n) Anexo 13 - Modelo de Ordem de Serviço (SEI nº 0131726);
o) Anexo 14 - Modelo de Termo de Compromisso de Manutenção de Sigilo (SEI nº 0131727);
p) Anexo 15 - Modelo de Termo de Ciência (SEI nº 0131728);
q) Anexo 16 - Modelo de Proposta Comercial (SEI nº 0127447); e
r) Anexo 17 - Modelo de Verificação de Soluções (SEI nº 0127448);

23. **DA SOLICITAÇÃO DA CONTRATAÇÃO E DA APROVAÇÃO**

23.1. Neste contexto, encaminhamos o Termo de Referência assinado pela Coordenação de de Infraestrutura de TI e Segurança da Informação - COINF para aprovação da Gerência de Tecnologia e Informação.

Aprovo o presente Termo de Referência e seus anexos em todo o seu teor, tendo em vista a coerência das justificativas e dos objetivos apresentados em relação à contratação em apreço.

Cleyton Domingues de Moura

Gerente de Tecnologia e Informação

Documento assinado eletronicamente por **Alessanderson de Castro Almeida**, **EPC - Integrante Técnico**, em 30/01/2024, às 17:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Eber Luis Barbosa Cherulli**, **EPC - Integrante Requisitante**, em 30/01/2024, às 17:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabiane de Sousa Dumont**, **Analista de Previdência Complementar**, em 31/01/2024, às 10:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.funpresp.com.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0141399** e o código CRC **33B9DF00**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 03750.010105.000005/2021-48 SEI nº 0141399

ANEXO 01 DO TERMO DE REFERENCIA

1. SERVIÇOS DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES

1.1. Tem por objetivo sustentar e operar as soluções de Antivírus e Firewall descritos neste termo, através de um catálogo de serviço pré-estabelecido pela Funpresp-Exe, anexo do presente termo, porém, não se limitando apenas a este. A CONTRATADA também deverá definir e realizar de forma periódica, ações proativas de acompanhamento de todo o parque, a fim de mantê-lo sempre estável, disponível e confiável.

Serviços de Operação e Resposta a Requisições		
Grupo de Serviço	**ID**	**Serviço**
Antivírus	1	Fornecimento de ferramenta de proteção de endpoints
	2	Gerenciamento centralizado dos clientes
	3	Instalação dos clientes via console/GUI
	4	Atualização de console/GUI
	5	Atualização dos Clientes via console/GUI
	6	Configuração de Políticas de proteção de endpoints
	7	Configuração de políticas de Firewall
	8	Configuração de Políticas de IPS
	9	Configuração de Políticas de Integridade do host
	10	Configuração de scans customizados
	11	Configuração de políticas de Controle de Aplicações e Dispositivos
	12	Criação de pacotes customizados para instalação do agente
	13	Configuração de políticas de grupo
	14	Configuração de integração (Servidores de Autenticação Suportados)
	15	Criação de Relatório de situação do parque (Atualização dos clientes)
	16	Configuração do método de autenticação de contas de administradores
Firewall	1	Configuração de política de segurança (L4/L7)
	2	Aplicação de política de Threat Prevention (antivírus, anti-spyware/bot ou IPS)
	3	Configurar integração com base de usuários (auth / AD)
	4	Aplicar controle de uso de aplicação por usuário/grupo de usuário
	5	Atualização firmware (SO)
	6	Criação de rota ou correção de tráfego assimétrico
	7	Configuração de PBF (Policy Based Forwarding)
	8	Aplicação de política de SSL Decryption
	9	Aplicação de categoria de URL filtering baseada em usuário/grupo de usuário
	10	Análise/criação de IOC (Indicator of Compromise)
	11	Criação de assinatura customizada para identificação e controle de aplicação
	12	Aplicação de políticas de QoS
	13	Health Check (relatório de adoção de uso de boas práticas de config)

1.2. Este serviço ainda tem por finalidade a responsabilidade de gerenciar todo o ciclo de vida de todas as requisições de serviços, referente aos serviços contratados visando:

1.2.1. Oferecer canais de comunicação integrados para funcionários autorizados do corpo técnico do CONTRATANTE requisitarem e receberem devolutivas de serviços pré-definidos, presentes no catálogo de serviços do presente instrumento.

1.2.2. Realizar mudanças padrões, pré-definidas e presente no catálogo de serviços do presente instrumento.

1.2.3. Receber reclamações e sugestões a respeito dos serviços prestados.

1.3. SOBRE O SISTEMA DE *ITSM* A SER UTILIZADO

1.3.1. Todas as requisições devem ser registradas, controladas, coordenadas, promovidas e gerenciadas por todo o seu ciclo de vida por meio de um único sistema. Isso garante uma abordagem consistente e reproduzível para o tratamento das requisições e reduz o potencial conflito, e a quantidade de requisições perdidas que possam surgir durante o tratamento.

1.3.2. Tal sistema de gestão e controle de requisições de serviço, deve ser do tipo ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI). O sistema de ITSM deve ser obrigatoriamente de propriedade da CONTRATADA, ser instalado em infraestrutura de propriedade da CONTRATADA.

1.3.3. Para que, em qualquer tempo e independentemente do local, os funcionários autorizados da CONTRATANTE tenham a possibilidade de abrir requisições para o CSOC (*Cyber Security Operations Center)* da CONTRATADA, o sistema de ITSM utilizado pela CONTRATADA, deverá ser acessível via internet utilizando protocolo criptográfico SSL, com certificado digital emitido em nome da CONTRATADA.

1.4. SOLICITANTES AUTORIZADOS E QUALIDADE DOS ATENDIMENTOS

1.4.1. Uma das origens de requisição de serviço poderá ser via interface humana e, a fim de evitar possíveis alterações anômalas e indesejadas no ambiente de segurança da informação, apenas funcionários autorizados pela CONTRATANTE poderão realizar abertura de requisições de serviços.

1.4.2. Sempre que uma nova requisição de serviço for solicitada pela CONTRATANTE, a CONTRATADA deverá previamente observar se tal contato está autorizado a solicitar tais serviços, antes de iniciar o atendimento. Caso tal contato não seja autorizado, o atendimento não deverá ser iniciado, e um comunicado de tentativa de abertura de atendimento não autorizado deve ser enviado ao gestor de contrato por parte do CONTRATANTE.

1.4.3. A CONTRATADA deverá manter uma plataforma para gerir tais contatos autorizados, constando ao menos as seguintes informações dos contatos: nome, telefone, e-mail, cargo. O gerenciamento (criar, atualizar, desativar e remover) desta plataforma deve estar disponível via internet para o CONTRATANTE, seguindo os critérios de segurança estabelecido para o sistema de ITSM, ou seja, acessível via internet utilizando protocolo criptográfico SSL, com certificado digital emitido em nome da CONTRATADA.

1.4.4. A plataforma de gestão de contatos autorizados deve ter a capacidade de relacionar os contatos autorizados, com os itens de configuração de sua responsabilidade do ambiente de segurança da informação do CONTRATANTE.

1.4.5. Nos primeiros 30 (trinta) dias do contrato, o CONTRATANTE informará à CONTRATADA quem e quantos são os contatos autorizados, bem como a matriz de responsabilidade relacionada aos itens de configuração que compõem a arquitetura de segurança da informação do CONTRATANTE.

1.4.6. Após o recebimento da informação, a CONTRATADA deverá disponibilizar os acessos aos canais de comunicação a todos os contatos autorizados em até 15 (quinze) dias. A CONTRATADA ainda deve enviar o comunicado de boas-vindas para cada contato, com manual de acesso a cada canal de comunicação, bem como também suas devidas credenciais.

1.4.7. O acesso aos canais de comunicação relacionado no presente termo, de qualquer tipo (telefonia, sistemas, e-mails) devem estar disponíveis para todos os contatos autorizados, a serem relacionados pelo CONTRATANTE, independentemente da quantidade.

1.4.8. No fechamento de toda e qualquer requisição de serviço, independente da severidade e/ou tempo de atendimento, a CONTRATADA deverá enviar uma pesquisa de satisfação para o solicitante. Tal pesquisa deve se basear no método NPS do inglês *Net Promoter Score.*

1.4.9. Caso a satisfação do atendimento avaliado for menor do que 70% (setenta por cento), um analista de qualidade da CONTRATADA deverá

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

entrar em contato com o requisitante do serviço, a fim de avaliar com mais detalhes as razões pelas quais o atendimento não alcançou a satisfação desejada.

1.4.10. Posteriormente um processo de não conformidade deve ser aberto, e em até 7 (sete) dias úteis, deve ser apresentado ao CONTRATANTE, um plano de ação de melhorias para que eventual insatisfação não volte a acontecer.

1.5. CENTRAL DE SERVIÇOS

1.5.1. Para atender ao determinado processo apresentado no tópico PROCESSO DE ATENDIMENTO PARA CUMPRIMENTO DE REQUISIÇÃO DE SERVIÇOS do presente termo, a CONTRATADA deverá possuir uma central de serviço, com o objetivo de proporciona um único ponto de contato para todos os funcionários do CONTRATANTE autorizados a realizar uma requisição de serviço.

1.5.2. Tal central terá acesso a dados e informações referente a arquitetura de segurança da informação do CONTRATANTE, e com o objetivo de manter tais acessos aos dados e informações sobre a governança e legislação brasileira, ambas as centrais de serviço devem obrigatoriamente serem instaladas fisicamente no Brasil.

1.5.3. Todas as requisições de serviços restringem-se aos itens de configurações descritos no tópico 1.1 do presente termo. Todos os itens de configurações fazem parte único e exclusivamente do ambiente de segurança da informação do CONTRATANTE, sendo assim toda e qualquer requisição de serviço estará ligada a tal ambiente, logo a central de serviço deve ser parte de um CSOC (*Cyber Security Operations Center*).

1.5.4. O CSOC deve obrigatoriamente ser de propriedade da CONTRATADA e deve possuir certificação ABNT NBR ISO/IEC 20000 ou ABNT NBR ISO/IEC 27001 em nome da CONTRATADA, não sendo permitido a terceirização ou subcontratação de tal ambiente físico e/ou serviço.

1.5.5. A CONTRATADA a qualquer tempo pode ser auditada pelo CONTRATANTE ou instituição independente definida pelo CONTRATANTE, referente aos itens de controle e normas estabelecidos na ABNT NBR ISO/IEC 20000 ou ABNT NBR ISO/IEC 27001 aplicada, portanto se espera que a CONTRATADA tenha evidências e experiência de execução da norma.

1.5.6. A CONTRATADA deverá seguir também as melhores práticas de mercado, conforme preconizado em pelo menos três das normas abaixo:

a) NBR ISO/IEC 9001

b) NBR ISO/IEC 20000

c) NBR ISO/IEC 20001

d) NBR ISO/IEC 27001

e) NBR ISO/IEC 27002

f) NBR ISO/IEC 27701

1.5.7. Também deverá apresentar o plano de adequação nos serviços, de acordo com a Lei Geral de Proteção de Dados (LGPD).

1.6. **PORTAL DE SEGURANÇA A INFORMAÇÃO**

1.6.1. Um portal de indicadores deverá ser disponibilizado ao CONTRATANTE deverá contemplar, no mínimo, os requisitos abaixo.

1.6.2. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês software as a service), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.

1.6.3. O portal deverá estar acessível a CONTRATADA via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.

1.6.4. A CONTRATANTE terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.

1.6.5. O portal deverá possibilitar a visualizar o status de segurança e monitoramento em tempo real.

1.6.6. Deverá disponibilizar para os usuários da CONTRATANTE, a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico está disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7. REQUISITOS DA FERRAMENTA DE PROTEÇÃO DE ENDPOINTS

1.7.1. A solução de Endpoint Detection e Response deverá ser fornecida, operada, suportada e customizada pela CONTRATADA;

1.7.2. O licenciamento deverá ser obrigatoriamente de propriedade da CONTRATADA e não poderá ser do tipo open source (software livre);

1.7.3. Deve ser implantado por meio de módulo agente a ser instalado nos endpoints;

1.7.4. O módulo deve possibilitar a investigação nos endpoints via console de gerenciamento centralizado, por meio de consultas customizadas que serão realizadas em todos os computadores com o módulo ativado;

1.7.5. Requerimentos Gerais da Solução

1.7.5.1. A solução oferecida deve ser independente de qualquer outra solução de segurança implementada ou a ser implementada. Todos os recursos necessários devem ser fornecidos na contratação.

1.7.5.2. Deve ser licenciada de modo a atender pelo menos 800 endpoints, incluindo estações de trabalho e servidores.

1.7.5.3. O gerenciamento da solução deverá ser feito na cloud do fabricante, via browser, não sendo aceitas soluções com gerenciamento on-premises.

1.7.5.4. Deve permitir gerar alertas das soluções integradas;

1.7.5.5. Permitir a exportação dos alertas através da própria console;

1.7.5.6. Permitir o agendamento de novos relatórios diariamente, semanalmente, mensalmente ou em período customizado;

1.7.5.7. Deve permitir e possuir APIs para facilitar a integração de outras soluções;

1.7.5.8. Receber os índices de comprometimento de todas as soluções integradas (Endpoint) e realizar trocas transparentes entre as mesmas, permitindo que uma detecção em um dos vetores, automaticamente seja implementada nas demais soluções, sem a necessidade de download de uma vacina ou novo pacote de inteligência;

1.7.5.9. Permitir bloqueio de artefatos com apenas uma única ação para todas as soluções do lote;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.5.10. Deve implementar a tecnologia de EDR (Endpoint Detection and Response) nos endpoints sem a necessidade de nenhum agente adicional.

1.7.5.11. A solução completa deve utilizar um único agente, incluindo todas as funcionalidades (Antivírus, Anti-Malware, EDR, Anti-APTs, etc.).

1.7.5.12. A implementação das funcionalidades de EDR não devem requerer a utilização de nenhuma console adicional.

1.7.5.13. Todos os agentes devem suportar a visualização de dados como:

a) Nome do usuário logado;

b) Nome do host;

c) Informações de sistema operacional (Build, Plataforma etc.);

d) Estado do equipamento (Online ou Offline);

e) Última data comunicação com a console de gerenciamento;

f) Informações relacionadas à rede (IP, DNS, DHCP etc.);

g) Timezone;

h) Versão do agente e todos os componentes;

i) Versão das definições de detecção;

j) Os usuários locais da plataforma devem ter uma política de senha que permita, no mínimo as seguintes configurações:

i. Alteração de senha após primeiro login;

ii. Definição do período de expiração da senha;

iii. Número mínimo e máximo de caracteres aos quais devem incluir letras maiúsculas, minúsculas e números;

iv. Evitar repetição de senha em curto período.

1.7.5.14. A solução deve permitir a criação de usuários com perfis para, no mínimo:

a) Administrador (sysadmin);

b) Administrador limitado;

c) Usuários de monitoramento;

d) Usuários de API.

1.7.5.15. A solução deve possuir de forma bem documentada suas APIs públicas, as quais podem ser utilizadas para futuras integrações.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.5.16. A solução deve possuir tecnologias de proteção contra ameaças avançadas e gerar alertas quando elas forem detectadas no ambiente.

1.7.5.17. A solução deve possuir capacidade para responder de forma efetiva durante as investigações realizadas pelo time de operações ou de resposta a incidente, provendo através de sua console centralizada capacidades para coleta de artefatos, análise de processos, isolamento de equipamentos, recursos para forense e etc.

1.7.5.18. A solução deve fornecer visibilidade abrangente que permitirá às equipes de segurança procurar, identificar e discernir rapidamente o nível de ameaças detectadas, além de possuir recursos de detecção e resposta para identificar, investigar e conter equipamentos de forma rápida e agilizar a resposta.

1.7.5.19. A solução deve possuir um console de gerenciamento centralizado para todos os agentes implantados.

1.7.5.20. O console de gerenciamento centralizado de terminais deve ter pelo menos as seguintes funcionalidades:

a) Permitir definir e gerenciar grupos de dispositivos, que devem ser definidos de forma estática ou por meio de um filtro lógico, com base nas características dos dispositivos que suportam a criação de combinações lógicas;

b) A solução deve ser capaz de detectar agentes duplicados ou inativos;

c) Deve fornecer acesso seguro ao console por meio de uma interface web HTTPS;

1.7.5.21. Deve gerenciar alertas antigos, permitindo a exclusão automática e\ou envio de alertas aos administradores;

1.7.5.22. O painel de controle da solução (dashboard) deve exibir pelo menos as seguintes métricas de detecção e contenção: Número de terminais com alertas, número total de alertas, número de indicadores separados por fonte de inteligência, número de coletas classificadas por estado e número de terminais em status de contenção / isolamento;

1.7.5.23. Todas as informações forenses geradas pelo equipamento devem poder ser analisadas no mesmo console, sem ter que acessar outro software adicional;

1.7.5.24. A solução deve poder enviar alertas por e-mail e HTTP/HTTPS para, no mínimo, os seguintes eventos:

a) Indicador de presença de malware;

b) Indicações de execução de malware;

c) Bloqueio de exploração;

d) Detecção de exploração.

e) O dashboard deve exibir pelo menos o número total de equipamentos monitorados e o número de equipamentos ativos por período.

f) O console deve oferecer todas as versões de agentes disponíveis;

g) Todas as atualizações do agente devem ser feitas exclusivamente no console central;

h) A frequência de atualização dos agentes no console central deve ser de pelo menos 5 minutos;

i) A frequência de atualização dos indicadores de comprometimento dos agentes no console central devem ser pelo menos a cada 60 segundos.

1.7.5.25. Caso existam agentes duplicados, a solução deverá criar um alerta e permitir a resolução do problema através de ações executadas no console de gerenciamento.

1.7.6. Requerimentos gerais do agente

1.7.6.1. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.

1.7.6.2. Uma solução baseada em agente deve ser fornecida para a proteção de ameaças de dia zero em ameaças que não utilizam assinaturas ou padrões como a principal forma de detecção e bloqueio de ameaças.

1.7.6.3. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.

1.7.6.4. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.

1.7.6.5. A solução deve fornecer a capacidade de executar análises forenses de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.

1.7.6.6. A solução deve fornecer a opção de análise investigativa e\ou forense em sua própria console de gerenciamento.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.6.7. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger, atualizar e ainda realizar análises forenses.

1.7.6.8. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.

1.7.6.9. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).

1.7.6.10. No caso de detecção um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.

1.7.6.11. A solução deve poder integrar-se automaticamente com outros equipamentos de proteção anti-malware, a fim de criar indicadores de comprometimento com base nas detecções feitas na navegação (rede) e no correio (email) analisado. Expandindo assim suas capacidades de Endpoint Protection e EDR para uma plataforma completa de análise contra APTs também na rede, email e\ou nuvem.

1.7.6.12. A solução deve poder quarentenar máquinas infectadas, isolando-as logicamente da rede sem afetar a capacidade de análise forense.

1.7.6.13. A solução deve implementar adicionalmente, as seguintes funcionalidades:

a) Rastreio de logons para detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.

b) Rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.

c) Rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.

d) Integração com sandbox para envio de artefatos suspeitos para análise.

e) Permitir que os administradores da solução se conectem remotamente aos dispositivos gerenciados, disponibilizando um terminal para execução de comandos do sistema operacional. Também deve ser possível o upload de scripts para execução.

f) Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa

artefatos, destacando rapidamente índices de comprometimento já conhecidos.

g) Permitir encaminhamento de log de eventos do Windows (Event Viewer) via syslog para soluções SIEM. Deve permitir, pelo menos, o envio dos seguintes tipos de logs do Windows: System, Application Experience, Security, AppLocker, PowerShell, Application, Windows Defender, Task Scheduler, Print Service, and Terminal Services.

h) Permitir a criação de alertas e, opcionalmente, bloqueios de ataques que visam bypass do controle de conta de usuário (UAC), identificando rapidamente atividades potencialmente maliciosas, gerando alertas para os hosts envolvidos. A funcionalidade deve detectar, minimamente, as seguintes técnicas de ataque: Token manipulation, Process masquerading, Environmental variable hijacking, Shell command hijacking, COM handler hijacking, Program output abuse.

1.7.6.14. A solução deve permitir a criação de exceção em caso de falso positivo ou até mesmo em casos pontuais para atendimento de possíveis regras do negócio.

1.7.6.15. A solução deve possuir módulos de detecção avançados, tais como mecanismos de machine learning e proteção contra exploração de vulnerabilidades em aplicações, também permitindo que exceções ou customizações de regras sejam realizadas para impedir falsos positivos ou até mesmo para atender regras do negócio.

1.7.6.16. A solução deve permitir a configuração de autoproteção como, configurar uma senha para impedir sua remoção por usuários não autorizados.

1.7.6.17. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.

1.7.6.18. A solução deve permitir a criação de grupos de hosts de forma estática, ou seja, adicionando manualmente todos os ativos pertinentes;

1.7.6.19. A solução deve permitir a criação de grupos de hosts dinâmicos, movimentando os ativos automaticamente, baseado minimamente nos seguintes critérios:

a) Versão do agente;

b) Domínio na qual a máquina está inserida ou grupo de trabalho;

c) Sistema operacional;

d) Arquitetura;

e) Timezone;

f) Subnet;

g) Hostname.

1.7.6.20. A solução deve permitir o cadastramento de hosts de alto valor, como Active Directory, Exchange, Banco de dados, etc, não permitindo que certas ações de resposta se apliquem aos mesmos.

1.7.6.21. A solução deve possuir capacidade de realizar ações tais como:

a) Coleta de arquivos;

b) Isolamento de hosts;

c) Obter listagem de arquivos da máquina;

d) Obter pacotes de diagnóstico para análise de saúde do agente;

e) Deletar alertas do host;

f) Coleta de comandos digitados em:

g) PowerShell;

h) CMD;

i) Bash.

1.7.6.22. A solução deve permitir a customização de ações, facilitando assim o tipo de coleta durante uma investigação.

1.7.6.23. A solução deve permitir a realização de análise das coletas através da console centralizada, sem necessidade de extrair estes dados durante a análise inicial.

1.7.6.24. Deve haver a possibilidade de importar indicadores ou mesmo criar indicadores customizados dentro da plataforma para que estes sejam utilizados para detecção e contenção de ameaças.

1.7.6.25. A solução deve permitir realizar buscas específicas sobre os eventos coletados e catalogados na console centralizada, assim como permitir a realização de buscas em tempo real de indicadores de comprometimento.

1.7.6.26. A plataforma deve submeter a rede de inteligência do fabricante todos os hashs de arquivos verificados pelos agentes, obtendo respostas rápidas sobre o nível de risco do artefato.

1.7.6.27. A solução deve realizar rastreamento de logons, permitindo a pesquisa por meio da interface gráfica da solução, possibilitando o rastreamento de máquinas acessadas por um determinado usuário.

1.7.6.28. O rastreamento de logons deve possuir inteligência para detecção de movimentação lateral e utilização indevida de credenciais.

1.7.7. Requerimentos técnicos do agente

1.7.7.1. Suportar a instalação em ambientes Windows, suportando minimamente:

a) Windows 7;
b) Windows 8;
c) Windows 10;
d) Windows Server 2008 R2;
e) Windows Server 2012;
f) Windows Server 2016;
g) Windows Server 2019.
h) MAC OS 10.15 +

1.7.7.2. Deve suportar distribuições Linux para no mínimo, as seguintes versões:

a) Red Hat Enterprise Linux (RHEL) 6.8 a 6.10;
b) Red Hat Enterprise Linux (RHEL) 7.1 a 7.7;
c) Red Hat Enterprise Linux (RHEL) 8;
d) CentOS 6.8 a 6.10;
e) CentOS 7.1 a 7.7;
f) CentOS 8;
g) Ubuntu 14.04, 16.04, 18.04, 19.04;
h) Oracle Linux 6.10, 7.6.

1.7.7.3. Deve suportar sistemas de 32 e 64 bits.

1.7.7.4. Agente único com mecanismos de detecção para minimizar a configuração e maximizar a detecção e o bloqueio.

1.7.7.5. A solução deve poder operar independentemente da localização da estação de trabalho, desde que esteja conectada à Internet.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.8. Capacidades técnicas mínimas necessárias:

1.7.8.1. Capacidade de detectar malware conhecido, incluindo vírus, cavalos de tróia, worms, spyware, adware, key loggers, rootkits e outros programas indesejados.

1.7.8.2. Detectar, possíveis incursões.

1.7.8.3. Responder, de forma a fazer a contenção e correção dos problemas.

1.7.8.4. A solução deve oferecer suporte ao uso de indicadores de comprometimento para detecção de presença e execução de malware. Os indicadores de compromisso devem ser fornecidos pelo fabricante e atualizados automaticamente e regularmente.

1.7.8.5. Deverá realizar rollback de ransomware para sistemas operacionais Windows, baseado em VSS

1.7.8.6. Os indicadores de comprometimento devem permitir identificar pelo menos as seguintes atividades de ameaças e/ou evidências:

a) Uso não autorizado de contas de usuário válidas;

b) Atividade de comando e controle;

c) Malware conhecido e desconhecido;

d) Tráfego de rede suspeito;

e) Uso de programas válidos para fins maliciosos;

f) Acesso não autorizado a arquivos do sistema.

1.7.8.7. A solução deve permitir a criação de indicadores de comprometimento manual e\ou automaticamente por meio de API ou manualmente no console de gerenciamento.

1.7.8.8. Os indicadores de compromisso devem permitir a avaliação de pelo menos as seguintes condições:

a) Gravação de arquivo, avaliando minimamente: Caminho completo, nome do arquivo, tamanho do arquivo, Hash md5, processo que o gravou, caminho para o processo executado e usuário que o escreveu.

b) Gravação no registro, avaliando minimamente: processo que o gravou, caminho para o processo executado, caminho para a chave, nome e valor do atributo e tipo de evento de gravação.

c) Nova conexão de rede, avaliando minimamente: IP remoto e local, porta remota e local, protocolo, processo que iniciou a conexão,

processo que a escreveu, rota para o processo executado e usuário associado ao processo.

d) Carregamento de imagem binária para execução, avaliando minimamente: processo executado, nome e caminho do executável, processo que o carregou (pai) e caminho do executável que o carregou.

e) Resolução de DNS por meio da API do sistema operacional, avaliando minimamente: nome do host resolvido, processo associado à resolução, caminho para o executável do processo e usuário associado ao processo.

f) Eventos relacionados a processos, avaliando minimamente: tipo de evento, processo executado, nome e caminho do executável, processo que o iniciou (pai), caminho para o executável do processo que o iniciou, hora de início, linha de comando usada e hash md5 do binário.

g) URL acessada em navegadores suportados, avaliando minimamente: nome do host, URL, método HTTP, User Agent, cabeçalho HTTP, IP remoto, porta local e remota, processo associado a requisição e caminho para o executável do processo associado.

1.7.8.9. A solução deve permitir definir uma lista branca de dispositivos com os quais a comunicação não será interrompida no caso de isolamento de máquinas comprometidas.

1.7.8.10. Toda vez que um host for contido (isolado), a solução deve permitir a customização da tela de bloqueio que o usuário irá receber ao tentar realizar suas atividades.

1.7.8.11. Para desbloquear hosts isolados, a solução deve permitir a utilização de códigos específicos, a serem obtidos na console de gerenciamento, a fim de validar a ação de resposta.

1.7.8.12. A solução deve suportar a capacidade de executar pesquisas em massa em toda ou parte da base instalada usando uma sequência de condições lógicas e operadores "e" / "ou". Os resultados dessas pesquisas devem retornar a lista de dispositivos pesquisados, se a pesquisa foi efetiva ou falhou e se ocorreu um erro durante a pesquisa

1.7.8.13. A detecção de uma exploração deve acionar automaticamente a coleta de evidências das atividades realizadas anteriormente pelo aplicativo afetado. As evidências devem ser armazenadas no servidor de gerenciamento e acessadas na console para análise profunda do alerta.

1.7.8.14. A solução deve suportar a criação de grupos de estações nas quais a execução da detecção de exploração é excluída.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.8.15. No caso de um alerta, a solução deve executar uma captura automática de recursos para análise forense. No mínimo, deve fornecer as seguintes informações:

a) Usuário conectado na estação de trabalho;

b) Conteúdo em cache;

c) Serviços em execução e portas abertas;

d) Contas de usuário e tarefas agendadas;

e) Processos em execução.;

f) Subconjuntos de registros de dados relacionados à atividade recente;

g) Dados do sistema;

h) Histórico e downloads do navegador;

i) Entradas DNS e ARP.

1.7.8.16. A solução deve fornecer uma API que permita a integração com outros produtos. A API deve ser adequadamente documentada para conhecer todas as operações possíveis e os valores e parâmetros necessários para utilização.

1.7.8.17. A API deve fornecer autenticação baseada em certificados digitais e deve ser acessada através de um protocolo SSL seguro.

1.7.8.18. A API deve oferecer suporte mínimo às seguintes opções: Criação, consulta, modificação e exclusão de todos os indicadores de comprometimento suportados pela solução. Consulta, listagem e exclusão de alertas gerados pela solução. Consulta de todas as estações de trabalho configuradas, consulta de detalhes de um host específico, criar aquisições de evidências, consultar as aquisições feitas e /ou exclui-las, manipular os processos de contenção de um host, criar um requisito de contenção, aprovar e restaurar um equipamento da contenção. Criar pesquisas para indicadores de consolidação em todas as estações de trabalho registradas.

1.7.8.19. A solução deve permitir que os agentes indiquem os IPs e os domínios que devem ser usados para a conexão ao console central e a ordem de prioridade em que devem tentar se conectar.

1.7.8.20. A solução deve permitir que os agentes usem uma configuração de proxy para se conectar ao console.

1.7.8.21. A solução deve incluir recursos de proteção baseados em malware conhecido e sua interação com os arquivos no sistema de arquivos. Qualquer arquivo malicioso deve ser isolado e armazenado em uma área de quarentena.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.8.22. A solução deve incluir scans de todos os arquivos no disco do dispositivo. Esses processos devem ser programáveis.

1.7.8.23. Os usuários devem ter a capacidade de interromper ou pausar os scans, mas esse recurso deve poder ser desativado pelo administrador.

1.7.8.24. Todos os requisitos de investigação devem ser listados juntamente com o status de execução, indicando se estão pendentes, em execução ou executados, bem como se algum erro foi detectado no processo.

1.7.8.25. A configuração da coleção deve permitir a inclusão de um ou mais dos seguintes componentes:

a) Gravação de arquivo, para no mínimo: caminho completo, nome do arquivo, tamanho do arquivo, hash md5, processo que o gravou, caminho para o processo executável, usuário que o escreveu;

b) Gravação no registro, para no mínimo: processo que o escreveu, caminho para o executável do processo, caminho para a chave, nome e valor do atributo e tipo de evento de gravação;

c) Conexão de rede, registrando-se minimamente: IP remoto e local, porta remota e local, protocolo, processo que iniciou a conexão, processo que a escreveu, rota utilizada pelo processo executado e usuário associado ao processo;

d) Carregamento de imagem binária para execução, para no mínimo: processo executado, nome e caminho do executável, processo que o carregou (pai) e caminho para o executável que o carregou;

e) Resolução de DNS por meio da API do sistema operacional, registrando minimamente: nome do host resolvido, processo associado à resolução, caminho para o executável do processo e usuário associado ao processo;

f) Eventos relacionados ao processo, para no mínimo: tipo de evento, processo executado, nome e caminho do executável, processo que o iniciou (pai), caminho para o executável do processo que o iniciou, hora de início, linha de comando usada e hash md5 do binário;

1.8. PROCESSO DE ATENDIMENTO PARA CUMPRIMENTO DE REQUISIÇÃO DE SERVIÇOS

1.8.1. A fim de balizar todo o processo de cumprimento de requisição de serviço do CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o

processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir.

1.8.2. Ao receber uma solicitação de requisição de serviço via e-mail ou telefone, de funcionários autorizados do CONTRATANTE, o analista da central de serviços deve registrar ou complementar as informações da requisição.

1.8.3. Para requisições de serviços abertas via web, o sistema de ITSM deve automaticamente realizar o registro da requisição de serviço.

1.8.4. Quando o requisitante realiza a requisição através de e-mail ou telefone, o analista da central de serviços, deve após registrar ou complementar a requisição, fazer a categorização e priorização da requisição de serviços.

1.8.5. A categorização deve ser realizada pelo analista da central de serviços relacionado o item de configuração, com o seu grupo definido no catálogo de serviços do Anexo 11. As demais informações levantadas devem ser documentadas na requisição de serviço.

1.8.6. Quando o meio de solicitação for via web o sistema de ITSM deve realizar a categorização e priorização da requisição de serviço automaticamente, obedecendo as mesmas regras seguidas pelo processo de registro via e-mail ou telefone.

1.8.7. A priorização deve ser realizada de acordo com as regras de negócio estabelecidas no anexo 10 - NÍVEIS MÍNIMOS DE SERVIÇO do presente termo.

1.8.8. Caso o analista da central de serviços não identifique o serviço solicitado como um item do catálogo de serviços, deverá este informar ao solicitante sobre sua inexistência. Na sequência o analista deve registrar uma solicitação de novo serviço ou modificação em serviço existente, que deve ser tratada pelo processo gerenciamento de portfólio do CONTRATANTE.

1.8.9. Uma vez identificado que o serviço requisitado consta no catálogo de serviços, e está disponível, o analista da central de serviços deve verificar se o serviço precisa ou não de aprovação para ser executado. Caso seja necessário, o analista deve submeter a requisição a um grupo aprovador.

1.8.10. O sistema de ITSM deve identificar automaticamente se o serviço é ou não elegível em primeiro nível, conforme configurado no catálogo de serviços.

1.8.11. Caso o serviço seja elegível para primeiro nível, o analista da central de serviço deverá atuar, desde que exista procedimento pré-estabelecidos e aprovados pelo CONTRATANTE.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.8.12. É de responsabilidade da CONTRATADA manter uma base de conhecimento com todos os procedimentos pré-estabelecidos e aprovados pelo CONTRATANTE. Tal base de conhecimento deve fazer parte do sistema de ITSM, e a qualquer tempo está acessível ao CONTRATANTE para consultas e aprovações de novos procedimentos.

1.8.13. Também é de responsabilidade da CONTRATADA a criação, revisão, manutenção, de tais procedimentos operacionais, sendo de responsabilidade do CONTRATANTE apenas participar como aprovador sempre que um procedimento for criado ou sofrer algum tipo de alteração.

1.8.14. Caso a solução da requisição de serviço dependa da atuação de um terceiro fornecedor do CONTRATANTE, o analista deve comunicar ao requisitante o status da requisição de serviço (pendente fornecedor), e o prazo previsto para o seu cumprimento. Nesse caso, a contagem do acordo de nível de serviço (SLA) é interrompido.

1.8.15. O analista da central de serviços que atuou no cumprimento da requisição deve fazer o registro da sua atuação, descrevendo informações relevantes para o cumprimento daquele serviço em particular.

1.8.16. Em caso de solução, o analista da central de serviços que atuou no cumprimento da requisição deve registrar no sistema de ITSM que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.

1.8.17. O analista da central de serviços, ao identificar que a requisição não é elegível em primeiro nível, deve encaminhá-la para o grupo solucionador indicado. Esse encaminhamento poderá ser automático, quando o grupo solucionador e a elegibilidade do serviço estiverem determinados no catálogo de serviços.

1.8.18. Ao receber uma requisição de serviço, o grupo solucionador deve analisá-la para verificar se compete ao grupo ou se deve ser encaminhada a outro grupo solucionador e, se para atendê-la, será necessária uma mudança.

1.8.19. Ao identificar que uma requisição de serviços encaminhada para a fila do grupo não faz parte do seu escopo, o analista do grupo solucionador deve redirecioná-la ao grupo mais indicado para atender a requisição. Se compete ao grupo solucionador, esse atua no cumprimento da requisição.

1.8.20. Caso seja necessária uma mudança para executar o serviço requisitado, o fluxo segue para o processo gerenciar mudanças. A governança sobre processo de gestão de mudança não pertence ao objeto deste termo, a

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

CONTRATADA apenas participará quando convocada do processo gestão de mudança já estabelecido pelo CONTRATANTE.

1.8.21. Se ao buscar atender à requisição de serviço o grupo solucionador identificar que para seu atendimento é necessário direcionar a solicitação a um fornecedor externo (de serviços ou de infraestrutura), deve acionar o fornecedor conforme as regras que serão estabelecidas pelo CONTRATANTE.

1.8.22. Nesse ponto, o status do chamado no sistema de ITSM deve ser atualizado para "encaminhado para fornecedor" e ficará aguardando seu retorno.

1.8.23. O registro da requisição de serviço na ferramenta do fornecedor, quando for o caso, deve ser documentado no registro da requisição no sistema de ITSM da CONTRATADA. Caberá ao grupo solucionador acompanhar e monitorar o fornecedor no atendimento da solicitação.

1.8.24. Cabe ao grupo solucionador avaliar e validar a entrega efetuada pelo fornecedor. São elementos de controle de qualidade e desempenho dessa atividade os níveis mínimos de serviço ou as regras definidas no instrumento contratual, edital de licitação e termo de referência.

1.8.25. O grupo que atuou no cumprimento da requisição de serviço deve fazer o registro da sua atuação no sistema de ITSM, descrevendo as informações relevantes para o cumprimento daquele serviço em particular.

1.8.26. Em caso de solução o grupo que atuou no cumprimento da requisição deve registrar no sistema de ITSM que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.

1.8.27. Após ser resolvida, a requisição de serviço deve ficar por 3 (três) dias corridos com status igual a resolvido, podendo ser reaberta pelo CONTRATANTE no determinado período, caso este entenda que tal requisição não foi resolvida de fato. Ao final de 3 (três) dias corridos, caso não haja nenhuma intervenção do CONTRATANTE, a requisição deverá ser alterada para o status fechada.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.9. ENTREGAS A SEREM REALIZADAS

1.9.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de requisições abertas	Soma de requisições abertas	Requisições abertas	Requisições	Número total de requisições abertas
Quantitativo de requisições concluídas	Soma de requisições concluídas	Requisições concluídas	Requisições concluídas	Número total de requisições concluídas
Quantitativo de requisições em backlog	Soma de requisições em backlog	Requisições em backlog	Requisições em backlog	Número total de requisições em backlog
TOP 10 – Ativos configurados	Soma do número de configurações por ativo	Requisições por ativo	Ativo	TOP do número de requisições por ativo
TOP 10 – Requisições por origem	Soma do número de requisições por origem	Requisições por origem	Origem	TOP do número de requisições por origem

1.9.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 02 DO TERMO DE REFERENCIA

1. SERVIÇOS DE GESTÃO DE VULNERABILIDADES

1.1. Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da Funpresp-Exe, a fim de evitar que ataques cibernéticos direcionados à Funpresp-Exe obtenham sucesso, explorando tais vulnerabilidades já conhecidas. Espera-se da CONTRATADA também suportar a CONTRATANTE nas correções de vulnerabilidade, quando estas forem identificadas nos equipamentos e soluções de segurança descritas no Anexo 12 – AMBIENTE FUNPRESP.

Serviços de Gestão de Vulnerabilidades		
Grupo de Serviço	**ID**	**Serviço**
Gestão de Vulnerabilidades	1	Checagem (scan) e varredura em ativos de rede
	2	Checagem (scan) e varredura em aplicações web
	3	Análise de falso positivo em ativos de rede
	4	Análise de falso positivo em aplicações web
	5	Informativo sobre vulnerabilidades em ativos de rede
	6	Informativo sobre vulnerabilidades em aplicações web
	7	Suportar correções das vulnerabilidades em ativos de rede
	8	Suportar correções das vulnerabilidades em aplicações web
	9	Apresentar abordagem dinâmica para priorizar correções

1.2. SOBRE AS ATIVIDADES DESEMPENHADAS

1.2.1. O serviço de descoberta de vulnerabilidades deverá contemplar, no mínimo, as seguintes atividades:

1.2.1.1. Preparação e realização de varreduras para análise de vulnerabilidades de ativos de infraestrutura de TI e aplicações Web e elaboração de relatório da análise;

1.2.1.2. Instalação, configuração e documentação das ferramentas fornecidas, inclusive suas integrações;

1.2.1.3. Apoio na manutenção preventiva, corretiva e atualizações das ferramentas fornecidas;

1.2.1.4. Gerar mensalmente relatório com serviços realizados no mês, vulnerabilidades não corrigidas e tempos de atendimento. O relatório mensal poderá ser customizado de acordo com a necessidade da Funpresp-Exe;

1.2.1.5. Identificar possíveis vulnerabilidades de segurança da informação, a fim de apoiar a definição de plano de ação mensal e evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;

1.2.1.6. A solicitação dos serviços será realizada por meio de chamado aberto pela FUNPRESP-EXE;

1.2.1.7. A CONTRATADA deve apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos.

1.3. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

1.3.1. As ferramentas e soluções utilizadas para prestação do serviço supracitado deverão ser agrupadas, a saber:

1.3.1.1. Deverá ser utilizada, pelo menos, 01 (uma) ferramenta de Gestão de Vulnerabilidades com foco em infraestrutura e aplicações web. A ferramenta deverá ser apresentada para ciência e aprovação em sua utilização, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades e não poderão ser baseadas em software livre.

1.3.1.2. Escaneamento, análise e gestão de vulnerabilidades: Soluções e ferramentas utilizadas pela CONTRATADA para realizar o processo de descoberta de novas vulnerabilidades de aplicações e infraestrutura, além de gerir todo ciclo de vida das vulnerabilidades encontradas, desde a sua descoberta até sua correta mitigação.

1.3.1.3. O processo de varredura e descoberta de vulnerabilidades, deverá ser executado na infraestrutura local, ou seja, na própria rede da CONTRATANTE. Após a coleta de dados de vulnerabilidades na infraestrutura da CONTRATANTE, esses dados poderão ser sincronizados com uma console de gerenciamento da solução em nuvem ou na infra local para análise;

1.3.1.4. A solução deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

1.3.1.5. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.1.6. Blindagem de vulnerabilidades em aplicações web: Soluções e ferramentas utilizadas pela CONTRATADA para realizar o processo de blindagem de vulnerabilidades conhecidas em sistemas web.

1.4. DESCOBERTAS DE VULNERABILIDADES

1.4.1. A CONTRATADA deverá compor ao ambiente de segurança da informação atualmente implementadas no CONTRATANTE, soluções de gestão de vulnerabilidades capazes de identificar vulnerabilidades de infraestrutura e aplicações, que possam comprometer a disponibilidade, integridades e confidencialidade dos dados e serviços do CONTRATANTE.

1.4.2. Para a prestação deste serviço deverão ser utilizadas ferramentas para descoberta de novas vulnerabilidades de aplicações e infraestrutura bem como a gestão de todo ciclo de vida das vulnerabilidades encontradas, desde a descoberta até a correta mitigação.

1.4.3. As soluções de prestação dos Serviços de Gestão de Vulnerabilidades deverão serem instaladas no CSOC e no CONTRATANTE, caso esse julgue ser necessário, de modo a prover varredura, identificação e gestão de vulnerabilidades do parque computacional do CONTRATANTE.

1.4.4. Apesar de ser necessário e permitido a utilização de ferramentas para descoberta de vulnerabilidades no ambiente do CONTRATANTE, se espera que a CONTRATADA se utilize também de métodos e técnicas assistidas, para identificar possíveis vulnerabilidades no ambiente do CONTRATANTE.

1.4.5. A fim de mitigar e prever possíveis impactos durante as rotinas de validação de vulnerabilidade, antes do início da execução do serviço, as ferramentas adotadas para execução deverão ser apresentadas ao time de segurança da informação do CONTRATANTE, que poderá ou NÃO aprovar a utilização destas.

1.4.6. Todas as ferramentas e soluções hardware e/ou software, deverão possuir os seguintes requisitos nativos, a saber:

1.4.6.1. Varredura e descoberta de vulnerabilidades para todos os equipamentos e softwares que compõem a solução de SERVIÇOS GERENCIADOS DE SEGURANÇA, bem como para todo o ambiente computacional do CONTRATANTE, ou seja, estações de trabalho, impressoras, dispositivos móveis, access points, switches, roteadores entre outros;

1.4.6.2. Licenciamento para atendimento de scan de 800 elementos, incluindo estações de trabalho, notebooks, switches, roteadores, access points,

servidores de rede, aplicações e imagens de container, servidores de aplicações, servidores de banco de dados, aceleradores de rede WAN e firewalls.

1.4.6.3. O licenciamento deverá ser realizado sem custo adicional e de forma flexível, ou seja, não limitado por módulo. Cada licença adquirida deverá possibilitar a utilização para qualquer um dos ativos do item anterior;

1.4.6.4. Deverá ser possível alterar o uso da licença entre os ativos acima. Caso haja algum prazo mínimo para esta mudança de uso de licenciamento, está deverá ser de no máximo 90 dias;

1.4.6.5. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

1.4.6.6. A solução deve possuir ferramentas e processos automatizados para monitorar: Uptime, Comportamentos anômalos e performance da plataforma;

1.4.6.7. A fabricante da solução deverá possuir ISO 27001;

1.4.6.8. Descobrir ativos que possuam endereço IP nas redes da CONTRATADA, sejam servidores de rede, máquinas virtuais, estações de trabalho, serviços de infraestrutura, aplicações, switches, dentre outros;

1.4.6.9. Agrupamento de eventos baseada em sistemas operacionais, endereços IP, nome DNS, nome NetBIOS, porta de serviços e vulnerabilidades;

1.4.6.10. Detecção de vulnerabilidades em sistemas operacionais, protocolos de rede, aplicações WEB, banco de dados e aplicações comerciais e ferramentas de produtividade;

1.4.6.11. Detecção de vulnerabilidades em ambiente Microsoft Windows, incluindo Hot Fixes, Service Packs, registros de sistema operacional, backdoors, trojans, malwares, ferramentas peer-to-peer, portas de serviço habilitadas e antivírus;

1.4.6.12. Detecção de vulnerabilidades em ambiente Linux, incluindo patches de segurança, monitoramento de logs de sistema e de aplicações;

1.4.6.13. Detecção de vulnerabilidades em bancos de dados SQL Server, My SQL/MariaDB e Postgres, servidores WEB Apache, Nginx e IIS, além de plataformas de serviços de aplicação (WildFly, JBOSS, Tomcat);

1.4.6.14. Detecção de vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

1.4.6.15. Varredura de ativos de modo intrusivo e não intrusivo;

1.4.6.16. Capacidade de selecionar e agrupar ativos encontrados, com possibilidade de incluir faixa de exclusão de endereços IP para varredura;

1.4.6.17. Capacidade de definir templates de configuração de scans e de agendamento de scans;

1.4.6.18. Capacidade de configuração de usuário e senha para realização de varredura autenticada de sistemas operacionais e aplicações;

1.4.6.19. Capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;

1.4.6.20. Geração de tickets para vulnerabilidades encontradas, permitindo marcar uma vulnerabilidade em determinado ativo como corrigida ou ignorada;

1.4.6.21. Recurso para acompanhamento da evolução das remediações de vulnerabilidades encontradas;

1.4.6.22. Integração com a base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);

1.4.6.23. Definição de, no mínimo, 3 (três) níveis de criticidade de vulnerabilidades;

1.4.6.24. Recurso de base de conhecimento com, no mínimo, 50.000 (cinquenta mil) assinaturas de vulnerabilidades, com atualização automática a partir do site do fabricante;

1.4.6.25. Apresentação de graduação de riscos, baseada em pontuação, que permite medir o nível de riscos dos recursos e sistemas encontrados;

1.4.6.26. Apresentação de procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualizações de software;

1.4.6.27. Levantamento e classificação de criticidade de ativos, baseada na importância do ativo e nas vulnerabilidades encontradas;

1.4.6.28. Configuração de frequência e periodicidade de varreduras na rede;

1.4.6.29. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan;

1.4.6.30. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

1.4.6.31. Apresentação de relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional da Funpresp-Exe em relação aos riscos de segurança em TI, contendo: hosts encontrados, topologia de rede, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;

1.4.6.32. Atualização automática de tabela de ativos monitorados, com suporte à ferramenta de gestão de incidentes detectados (baseline), contendo informações sobre serviços e vulnerabilidades encontradas por ativo;

1.4.6.33. Recurso de alertas por e-mail de vulnerabilidades encontradas;

1.4.6.34. Capacidade de exportação de relatório de vulnerabilidades em formato PDF e CSV;

1.4.6.35. Gerenciamento por CLI (Commandline interface), SSH (Secure Shell), WebUI (WEB User Interface) via HTTPS (Secure Hypertext Transfer Protocol) e console gráfica centralizada;

1.4.6.36. Gerenciamento único, centralizado, virtualizável, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;

1.4.6.37. Gerenciamento por meio de software a ser instalado em ambiente virtualizado do CONTRATANTE;

1.4.6.38. Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios, permitindo também a visualização de status de serviços;

1.4.6.39. Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, throughput e desempenho dos serviços;

1.4.6.40. Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;

1.4.6.41. Gerenciamento com recurso de validação de políticas de segurança antes da aplicação, responsável pela identificação de erros e inconsistências;

1.4.6.42. Gerenciamento com recurso de replicação de configurações e atualização de software;

1.4.6.43. Gerenciamento com recurso de monitoramento de logs;

1.4.6.44. Gerenciamento com recurso de backup e importação automática de arquivos de configuração;

1.4.6.45. Analisar semanalmente os sites dos portais da Funpresp-Exe, com aproximadamente 100 páginas WEB, contra pichação (defacement) e ataques, tais como, mas não se limitando a, cross-site scripiting, SQL injection e DoS. É necessário atentar que essa lista poderá sofrer acréscimos ou supressões em virtude de mudanças no ambiente da CONTRATANTE.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.4.6.46. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades, utilizando no mínimo os seguintes critérios:

a) CVSS Impact Score;
b) Existência de códigos de exploração da vulnerabilidade encontrada (exploit);
c) Existência de módulos de exploração da vulnerabilidade em frameworks automatizados, tais como: Metasploit, Core Impact, CANVAS.

1.4.6.47. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades;

1.4.6.48. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

a) CVSSv3 Impact Score;
b) Idade da Vulnerabilidade;
c) Se existe ameaça ou Exploit que explore a vulnerabilidade;
d) Número de produtos afetados pela vulnerabilidade;
e) Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;
f) Lista de todas as fontes (canais de mídia social, Dark Web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;

1.4.6.49. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas como também de fontes não gratuitas;

1.4.6.50. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:

a) Endereço IPv4 e IPv6, quando aplicável;
b) Sistema Operacional;
c) Nome NetBIOS;
d) FQDN;

1.4.6.51. A solução deve incluir a capacidade de programar períodos onde varreduras não podem ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, etc), hora de inicio e fim da janela, quais ativos serão excluídos e o fuso horário do agendamento;

1.4.6.52. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é Nova, Persistente, Corrigida ou Reapareceu no ativo;

1.4.6.53. Deverá ser possível aceitar uma vulnerabilidade, onde a mesma não irá mais aparecer na console. Este processo poderá ser feito para um único ativo

ou múltiplos ativos. Ainda, deverá ser possível definir uma data de expiração para a Aceitação.

1.5. PLATAFORMA DE GESTÃO DE VULNERABILIDADE EM APLICAÇÕES WEB

1.5.1. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

1.5.2. A solução deverá capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS);

1.5.3. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

1.5.4. Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

1.5.5. Deve possui modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados;

1.5.6. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

1.5.6.1. Cookies, headers, formulários e links;

1.5.6.2. Nomes e valores de parâmetros da aplicação;

1.5.6.3. Elementos JSON e XML;

1.5.6.4. Elementos DOM;

1.5.7. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

1.5.8. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

1.5.9. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

1.5.10. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

1.5.11. Deve ser capaz de instituir no mínimo os seguintes limites:

1.5.11.1. Número máximo de URLs para crawl e navegação;

1.5.11.2. Número máximo de diretórios para varreduras;

1.5.11.3. Número máximo de profundidade dos elementos DOM;

1.5.11.4. Tamanho máximo de respostas;

1.5.11.5. Limite de requisições de redirecionamentos;

1.5.11.6. Tempo máximo para a varredura;

1.5.11.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

1.5.11.8. Número máximo de requisições HTTP por segundo;

1.5.12. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

1.5.12.1. Limite em segundos para timeout de requisições de rede;

1.5.12.2. Número máximo de timeouts antes que a varredura seja abortada;

1.5.12.3. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

1.5.12.4. Deve ser capaz de enviar notificações através de no mínimo e-mail;

1.5.12.5. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

1.5.12.6. Deverá avaliar sistemas web utilizando frameworks modernos, como AJAX, HTML5 e SPA;

1.5.12.7. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

1.5.12.8. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger)

1.5.12.9. Deverá suportar no mínimo os seguintes esquemas de autenticação:

a) Autenticação básica (digest);

b) NTLM;

c) Formulário de login;

d) Autenticação de Cookies;

e) Autenticação através de Selenium ou outro similar;

1.5.12.10. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.5.12.11. Deve ser capaz de customizar parâmetros como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

1.5.12.12. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;

1.5.12.13. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

1.5.12.14. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

1.5.12.15. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

1.5.12.16. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

a) Payload injetado;

b) Evidência em forma de resposta da aplicação;

c) Detalhes da requisição HTTP;

d) Detalhes da resposta HTTP;

1.5.12.17. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

1.5.12.18. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

1.5.12.19. A solução deve possuir suporte a varreduras de componentes para no mínimo: AngularJS, Apache, Apache Tomcat, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, jQuery, Lighttpd, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI.

1.5.12.20. A solução deverá possuir controle de permissão de usuários, com no mínimo menos 3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura.

1.5.12.21. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução.

1.5.12.22. A solução deverá possuir um Add-on para o navegador que permita gravar uma macro de autenticação para criação do Selenium ou outra solução similar.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.5.12.23. Deverá ser possível excluir a interação com elementos DOM durante o scan. Está exclusão poderá ser configurada para cada elemento, sendo possível escolher o conteúdo do texto ou do atributo CSS.

1.5.12.24. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pela console de gerência.

1.5.12.25. Deve ser possível alterar o user agent utilizado pela solução.

1.5.12.26. A solução deve suportar listas de exclusão globais.

1.5.12.27. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes.

1.5.12.28. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas.

1.5.12.29. Deve ser possível gerar relatório das vulnerabilidades, no mínimo em PDF, HTML e CSV.

1.6. PLATAFORMA DE GESTÃO DE VULNERABILIDADE EM CONTÊINERES

1.6.1. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

1.6.2. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

1.6.3. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;

1.6.4. A solução deve ser capaz de se integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do CONTRATANTE com a finalidade de evitar o envio de imagens e propriedade intelectual da CONTRATANTE;

1.6.5. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

1.6.6. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

1.6.7. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

1.6.8. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção;

1.6.9. A solução deve analisar as camadas (layers) de um container;

1.6.10. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

1.6.11. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas;

1.6.12. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

1.6.13. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

1.6.14. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

1.6.15. A solução deve possuir conectores e permitir importação de imagens dos repositórios disponíveis na infraestrutura da CONTRATANTE de acordo com o ANEXO 12 – AMBIENTE DA FUNPRESP

1.6.16. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor, Sonatype Nexus e Google Cloud Plataform para importar e analisar imagens;

1.6.17. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE;

1.6.18. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

1.6.19. Caso a condição da política seja verdadeira, a solução deve ser capaz de prevenir o pull destas para implementação ou identificar a falha de compliance das imagens para ação do time de segurança;

1.6.20. A solução deve permitir a criação de políticas especificas por repositório;

1.6.21. A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernets;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.6.22. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser:

1.6.22.1. Nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a container, algumas já explicitadas em itens anteriores, e já licenciada para uso.

1.7. BLINDAGEM DE VULNERABILIDADES EM APLICAÇÕES WEB

1.7.1. Todas as ferramentas e soluções deverão ser fornecidos em nuvem e deverão possuir os seguintes requisitos nativos, a saber:

1.7.1.1. Não intrusiva, ou seja, não ter a necessidade de instalação de agentes ou outros softwares nos servidores da CONTRANTATE.

1.7.1.2. Plataforma deve ser hospedada fora da estrutura da CONTRATANTE, em estrutura de nuvem pública.

1.7.1.3. O ponto de presença no Brasil deve ser capaz de processar todos os requisitos abaixo apresentados.

1.7.1.4. Disponibilização de uma plataforma na internet como ponto único de comunicação da infraestrutura de origem de órgão com o “mundo externo” para tráfego HTTP e HTTPS.

1.7.1.5. A plataforma deve garantir 99,99% de disponibilidade/nível de serviço anual (SLA);

1.7.1.6. Capaz de identificar indisponibilidades de rota de forma automática, alterando-as se necessário, para maximizar a disponibilidade do conteúdo no browser do usuário;

1.7.1.7. A Plataforma de proteção deve garantir alto desempenho de acesso (baixo tempo de carga das páginas) independentemente de quantidade de usuários e de dados acessados simultaneamente, apresentando delay máximo de 500 milissegundos;

1.7.1.8. A Plataforma de proteção deve disponibilizar ferramenta para monitoramento real das informações dos usuários, a partir dos servidores de borda da própria rede de distribuição.

1.7.1.9. A Plataforma de proteção deve prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável,

automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos;

1.7.1.10. A plataforma deverá disponibilizar meios de notificação de alertas das seguintes categorias:

a) Quando sites são adicionados ou removidos da plataforma
b) Notificação em tempo real de ataques ocorrendo nas aplicações protegidas pela plataforma.
c) A plataforma deve permitir a criação de usuários com perfis de acesso distintos.
d) A plataforma deve possuir logs administrativos de todas as alterações realizadas pelos administradores.

1.7.1.11. A plataforma deve possuir Dashboard acessível através de Browser o qual permita:

a) Analisar o histórico de tráfego (hits, requisições e throughput por segundo);
b) Analisar alertas e configurações das políticas de segurança;
c) Analisar em tempo real as requisições recebidas pela plataforma, distinguindo a porcentagem de tráfego real e malicioso bem como a porcentagem de tráfego sendo provido pelo cache.
d) Analisar o log de requisições legitimas e maliciosas que acessaram a plataforma.

1.7.1.12. As configurações realizadas pelos administradores devem ser propagadas instantaneamente para todos os datacenters da plataforma.

1.7.1.13. A defesa da solução deve disponibilizar que todos os servidores da Plataforma de proteção sejam capazes de monitorar, alertar e impedir atividades maliciosas direcionadas aos servidores da FUNPRESP-EXE através de um Web Application Firewall;

1.7.1.14. A solução deverá ter recursos avançados de geração de relatórios claros, de fácil entendimento e atender à conformidades regulatória, permitindo gerar relatórios personalizados ou pré-definidos.

1.7.1.15. A defesa da solução deve ser capaz de correlacionar ataques com precisão, por meio da competência de aprender todos os aspectos do aplicativos WEB, incluindo diretórios, URLs, parâmetros e entrada de usuários aceitáveis, bem como a validação de ataques correlacionando e analisando as violações de forma individuais ou combinadas para detectar ataques com maior precisão e bloquear apenas tráfego malicioso tendo como finalidade a minimização de falsos positivos.

1.7.1.16. A defesa da solução deve ser capaz de filtrar e proteger os ataques direcionados a vulnerabilidade da aplicação, respeitando os padrões da

indústria sendo capaz de identificar, alertar e impedir que o acesso malicioso seja realizado, garantindo no mínimo o bloqueio dos grupos de regras listadas, independente do volume:

a) Violação por anomalias de protocolo, incluindo inexistência do header na requisição;
b) Bloqueio de tentativas de SQL Injection
c) Bloqueio de tentativas de Cross Site Script
d) Bloqueio de Command Injections
e) Bloqueio de acesso de Trojan
f) Bloqueio de Backdoors

1.7.1.17. A defesa da solução deve ser capaz de proteger os ataques direcionados à camada de aplicação, alertando e/ou bloqueando por acessos excessivos de um único requisitante ou IP, antes que o acesso chegue a infraestrutura de origem possibilitando aplicar as seguintes regras:

a) Identificação do acesso para alerta e/ou bloqueio através do IP do usuário;
b) Identificação do acesso para alerta e/ou bloqueio através da sessão do usuário;
c) Identificação do acesso para alerta e/ou bloqueio através do cruzamento de IP do usuário e um determinado User Agent específico.
d) Identificação do acesso para alerta e/ou bloqueio de requisições com cabeçalhos excessivos.

1.7.1.18. A defesa da solução deve ser capaz de possibilitar ferramenta online para bloqueio ou permissão de IPs específicos desejados pela FUNPRESP-EXE;

1.7.1.19. A plataforma deve possuir linguagem de programação intuitiva e simples para a construção de políticas de segurança mais complexas.

1.7.1.20. A plataforma deve conter mecanismos de proteção e mecanismos de alertas tais como:

a) Proteção antibot.
b) Proteção contra ataques na Web de dia zero
c) TCO reduzido com mais baixos falsos positivos
d) Dispositivo de prevenção de DDoS
e) Comportamento Profundo Baseado em Intenção Análise
f) Cobertura total das ameaças automatizadas da OWASP
g) Proteger todos os canais: aplicativos Web e móveis, APIs

1.7.1.21. Este tipo de proteção não deve fornecer proteção baseada apenas em assinaturas, mas também possuir modelos de segurança positivos e/ou detecção de anomalia.

1.7.1.22. A Plataforma deve permitir que as regras estejam em alerta ou bloqueio;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.1.23. A plataforma deve realizar a análise dos IPs requisitantes protegendo as aplicações de serem acessadas pelas seguintes origens: rede TOR, proxies anônimos e endereços IP de baixa reputação.

1.7.1.24. A plataforma deve proteger as contas de usuários das aplicações contra ataques.

1.7.1.25. A solução deverá integrar-se com a maioria dos principais sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM). Deverá conter com a possibilidade de exportar eventos como mensagens syslog, formato Common Event Format (CEF) e formato JSON, permitindo pesquisas para rápidas respostas a possíveis incidentes e intuitivamente indexados.

1.7.1.26. A solução contratada, deverá permitir a integração, manual ou automática, de regras resultantes das análises de vulnerabilidade periódicas a serem executadas de acordo com a frequência quando houver necessidade de análise das URLs por parte da CONTRANTE.

1.7.1.27. A plataforma de posse dos resultados do scanner de vulnerabilidade, deverá aplicar “patches virtuais” nas aplicações vulneráveis, de forma a protegê-la de ataques.

1.7.1.28. A CONTRATADA deverá prestar o treinamento inicial da solução (hands-on), observando os seguintes critérios:

a) Treinamento para até 8 pessoas;
b) Duração mínima de 24 horas
c) Deve ter em sua ementa minimamente:
    i. Topologia da Solução
    ii. Portal de Monitoramento
    iii. Customização básica
    iv. Definição/montagem de regras
    v. Visualização dos Painéis
    vi. Customização dos Painéis
    vii. Criação de Relatórios
    viii. Geração de Relatórios

1.7.1.29. A CONTRATADA deverá prestar assistência técnica de atendimento 24 (vinte e quatro) horas x 7 (sete) dias por semana;

1.7.1.30. Deverá contemplar o monitoramento do ambiente onde a solução de WAF estiver sendo executada, evitando perdas de performance que possam prejudicar o serviço contratado.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.1.31. Dentre as possiblidades de chamados técnicos devem estar contemplados: Apoio a configurações, Criação de Regras, Refinamento de Regras, Customização de Relatórios e Resolução de problemas;

1.7.1.32. A CONTRATADA deverá licenciar e disponibilizar recursos adequados, conforme detalhamento:

a) Throughput de até 50 Mbps
b) Proteção de até 30 URLs

1.8. PROCESSO DE ATENDIMENTO PARA GESTÃO DE ANÁLISE DE VULNERABILIDADE

1.8.1. A fim de balizar todo o processo de gestão de vulnerabilidade do CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

1.8.2. O CONTRATANTE deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato, e deverá conter as seguintes informações mínimas, a saber:

a) Nome do ativo e/ou serviço;

b) Grupo de serviço;

c) IP;

d) Janela de análise (Horário permitido para análise);

e) Prioridade.

1.8.3. A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional do CONTRATANTE, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado ao CONTRATANTE.

1.8.4. De acordo com as variáveis e critérios estabelecidos no catálogo de serviços, na lista de ativos e recursos do CONTRATANTE, a CONTRATADA deverá realizar checagens (scans) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da FUNPRESP-EXE, utilizando as ferramentas e soluções definidas no presente termo de referência.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.8.5. Após o término das rotinas de checagens (scans) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas ao CONTRATANTE apenas vulnerabilidades que existam de fato em seu ambiente.

1.8.6. Após análise de falso positivo, a CONTRATADA deverá informar ao CONTRATANTE as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no tópico ENTREGAS A SEREM REALIZADAS do presente termo de referência.

1.8.7. Cabe única e exclusivamente ao CONTRATANTE liberar e/ou autorizar toda e qualquer mudança, sugerida para contenção e mitigação de uma vulnerabilidade encontrada. Sendo assim, nenhuma mudança deve ser realizada sem que antes haja a liberação da mesma pelo CONTRATANTE.

1.8.8. Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA apenas as correções de vulnerabilidades encontradas no ambiente listado no tópico Anexo 13 – AMBIENTE FUNPRESP obrigatoriamente obedecendo as definições proposta pelo comitê de mudança do CONTRATANTE.

1.8.9. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno que, para aplicá-las ao ambiente deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.

1.8.10. Como último passo a CONTRATADA deverá atualizar todos os controles e indicadores, estabelecidos no tópico ENTREGAS A SEREM REALIZADAS.

1.8.11. O processo descrito é mínimo esperado a ser seguido e executado pela CONTRATADA. Todavia, como o objeto do presente termo de referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria continua, a qual pode ser alterado desde que aprovado pelo CONTRATANTE.

1.8.12. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente, descrita no catálogo de serviços definido e detalhado na Seção destas especificações. O início do processo não se limita apenas em rotinas de tempo pré-definidas no catálogo de serviços, mas poderá o CONTRATANTE também solicitar análises sobre demanda a qualquer tempo.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 201/202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.9. ENTREGAS A SEREM REALIZADAS

1.9.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades identificadas	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades por severidade e por área responsável	Soma de vulnerabilidades de severidade por área responsável	Vulnerabilidades de severidade	Vulnerabilidades	Número total de vulnerabilidades de severidade por área responsável
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB	Soma de vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB

1.9.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

ANEXO 03 DO TERMO DE REFERENCIA

1. SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

1.1. Tem por objetivo o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à Funpresp-Exe, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura da Funpresp-Exe, que possam gerar eventos de segurança da informação, os quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo a um processo cíclico e rigoroso de gestão de eventos.

Serviços de Monitoramento de Ataques Cibernéticos		
Grupo de Serviço	**ID**	**Serviço**
Monitoramento de Ataques Cibernéticos	1	Eventos de Informação
	2	Eventos de Aviso
	3	Eventos de Exceção

1.2. SOBRE AS ATIVIDADES DESEMPENHADAS

1.2.1. O serviço de monitoramento e resposta a incidentes deverá contemplar as seguintes atividades:

1.2.1.1. Monitorar os eventos recebidos pelo sistema de correlação de eventos de segurança da informação;

1.2.1.2. Investigar os eventos recebidos para determinar se eles geraram incidentes de segurança da informação;

1.2.1.3. Classificar e tratar os incidentes identificados de acordo com os roteiros de operação;

1.2.1.4. Analisar as causas e os impactos dos incidentes tratados e propor controles para evitar novos incidentes similares;

1.2.1.5. Ser responsável pela gestão e documentação dos casos de uso configurados na ferramenta de monitoração e detecção;

1.2.1.6. Criar casos de uso configurando regras, limiares e alertas de acordo com as especificações fornecidas pela FUNPRESP-EXE;

1.2.1.7. Criar casos de uso configurando regras, limiares e alertas de acordo com as especificações desenvolvidas por equipe especializada da CONTRATADA com base em ameaças identificadas em outros clientes;

1.2.1.8. Aperfeiçoar as regras, limiares e alertas do sistema de correlação de eventos de segurança da informação, visando reduzir o número de falsos positivos e falsos negativos;

1.2.1.9. Apoiar a construção e melhoria de roteiros para tratamento de incidentes similares para formar uma base de conhecimento da FUNPRESP-EXE;

1.2.1.10. Criar dashboards nas ferramentas fornecidas para atendimento do serviço de acordo com as especificações fornecidas pela FUNPRESP-EXE;

1.2.1.11. A solicitação dos serviços de criação e customização de regras e dashboards específicos para a FUNPRESP-EXE será realizada por meio de chamado;

1.2.1.12. Instalação, configuração e documentação das ferramentas fornecidas, inclusive suas integrações;

1.2.1.13. Apoio na manutenção preventiva, corretiva e atualizações das ferramentas fornecidas;

1.2.1.14. Gerar mensalmente relatório com principais eventos de segurança identificados, incidentes tratados e tempos de atendimento. O relatório mensal poderá ser customizado de acordo com a necessidade da FUNPRESP-EXE.

1.3. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

1.3.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento de Logs e Pacotes que atendam o descritivo técnico a seguir.

1.3.2. A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar 2.500 eventos por segundo ou 300 gigabytes/dias, considerando que cada evento terá em média 1000 bytes de informação.

1.3.3. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de automático de máquina “Machine Learning” e deve contar com casos de uso para detectar ameaças avançadas;

1.3.4. A plataforma deverá possuir as características a seguir:

1.3.4.1. Deverá ser escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período;

1.3.4.2. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.4.3. Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.

1.3.4.4. A solução deve estar classificada como líder no quadrante mágico de "Security Information and Event Management" do Gartner em 2021;

1.3.4.5. A solução deve ter recursos de "Multi-tenant";

1.3.4.6. Deve ter as certificações SOC 2 TYPE II e ISO 27001;

1.3.4.7. Deve garantir retenção dos logs conforme arquitetura abaixo:

a) 7 dias hot retention;

b) 90 dias warm retention;

c) 365 dias cold retention.

1.3.4.8. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

1.3.4.9. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;

1.3.4.10. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

1.3.4.11. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

1.3.4.12. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;

1.3.4.13. Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar a reter dados por períodos estabelecidos para fins de conformidade e investigação;

1.3.5. A solução deve atender as seguintes características:

1.3.5.1. Deve oferecer suporte a integração com várias fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Google Cloude, SVN, Office 365, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow e sFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

1.3.5.2. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem,

permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;

1.3.5.3. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

1.3.5.4. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskope, ServiceNow, entre outros.

1.3.5.5. Deve ter uma interface que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;

1.3.5.6. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

1.3.5.7. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias possibilitando a integração entre aplicações (ambiente interno e externo);

1.3.5.8. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

1.3.5.9. Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:

a) Identidade do usuário;

b) Contexto de negócios

c) Metadados de ativos;

d) Informações de rede;

e) Localização Geográfica;

f) Dados de inteligência de ameaças;

1.3.5.10. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:

1.3.5.11. Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.5.12. Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;

1.3.5.13. Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;

1.3.5.14. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período;

1.3.5.15. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

1.3.5.16. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

1.3.5.17. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);

1.3.5.18. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

1.3.5.19. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;

1.3.5.20. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;

1.3.5.21. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;

1.3.5.22. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;

1.3.5.23. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

1.3.5.24. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;

1.3.5.25. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, etc;

1.3.5.26. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

1.3.5.27. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;

1.3.5.28. Deve ter relatórios de resumo executivo de violações, incidentes e operações;

1.3.5.29. Deve ter relatórios sobre a atividade do usuário;

1.3.5.30. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;

1.3.5.31. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

1.3.5.32. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir: I - Analisar mais de 1000 indicadores comportamentais de um artefato; II - Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não; III - Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

1.3.5.33. Para monitoramento de pacotes a CONTRATADA deverá fornecer recursos de NDR (detecção e resposta de rede) abertos (Metadados, Extração de arquivos/carvagem & assinatura baseado em IDS em uma única plataforma de aparelho) e :

a) Deve ser capaz de suportar mais de 35 protocolos de rede;

b) Deve ser capaz de fornecer timestamping nanossegundo baseado em FPGA de pacotes de rede capturados para permitir a pivotação e correlação rápida entre os registros de protocolo;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

c) Deve ter detecção de protocolo dinâmico para inspecionar cada pacote individualmente, negando de forma confiável as medidas de evasão;

d) A solução deve detectar tráfego de rede maliciosa potencial, como consultas de DNS para C&Cs botnet;

e) Deve ser criptografado a Coleta de Tráfego para capturar evidências e insights vitais de tráfego em certificados SSL, SSH e x509;

f) Deve ser capaz de detectar ataques de força bruta;

g) Deve ser capaz de detectar adivinhação credencial;

h) Deve ser capaz de transmitir registros bro / Zeek para:

i. Splunk

ii. QRadar

iii. Arcsight

iv. Elástico

v. CADA

vi. Securonix

vii. Exabeam

viii. FireEye

ix. Humio

x. Google Chronicle

xi. Kafka

xii. JSON sobre TCP

xiii. Amazon S3

xiv. Syslog

xv. SFTP

1.3.5.34. Para o dimensionamento da solução de NDR, pode ser considerado um valor mínimo de 2 Gbps de Throughput.

1.4. PROCESSO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

1.4.1. A fim de balizar todo o processo de monitoramento de ataques cibernéticos do CONTRATANTE, e influenciado pelos

principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

1.4.2. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.

1.4.3. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA, o CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva, porém se ratifica que é de responsabilidade da CONTRATADA a definição e colocar em operação tal linha de base.

1.4.4. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados ao CONTRATANTE sejam detectados através dos serviços em questão.

1.4.5. O produto de um evento é a correlação dos insumos: logs e rede, gerados pelos itens de configurações do parque do CONTRATANTE. Uma vez definido a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta definida no tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS.

1.4.6. Caso a CONTRATADA identifique a ausência dos insumos (logs de rede) a ser gerado por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no Anexo 12 – AMBIENTE FUNPRESP, respeitando a quantidade de Eventos Por Segundo – EPS contratado. Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar ao CONTRATANTE a correção e/ou habilitação de tal insumo no item de configuração em questão.

1.4.7. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos,

logo tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

I. **Eventos de Informação:** Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo identificar se as ferramentas e soluções, estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como por exemplo, *porcentagem de hosts com a última vacina de antivírus do dia.*

II. **Eventos de Aviso:** Este grupo de eventos deve ser utilizado, quando existe algum comportamento anômalo se comparado a linha de base de operação padrão do ambiente (serviço, trafego e/ou solução), porém ainda não gerou algum tipo de impacto ao ambiente (serviço, trafego e/ou solução) do CONTRATANTE, como por exemplo fictício: Por exemplo, *é esperado que exista 1000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém na última hora este número passou para 10000 (dez mil) ataques, todavia o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, trafego e/ou solução).*

III. **Eventos de Exceção:** Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e confidencialidade), foram impactados, *como por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus do CONTRATANTE.* Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, Anexo 04 do presente termo de referência.

1.4.8. Uma vez classificado o evento se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

I. **Para eventos do tipo Informação,** não é requerido qualquer tipo de ação, porém como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança, portanto se espera que a CONTRATADA os utilize para tal.

II. **Para eventos do tipo Aviso,** deve existir a garantia por parte da CONTRATADA que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomando as ações cabíveis para identificar a causar raiz da mudança de comportamento do ambiente.

III. **Para eventos do tipo Exceção,** deverá a CONTRATADA transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação, definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no Anexo 04 do presente termo de referência. Após a abertura do incidente de segurança obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

1.4.9. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

1.4.10. Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.5. ENTREGAS A SEREM REALIZADAS

1.5.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos/pacotes correlacionados por regra de correlacionamento	Eventos e pacotes correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos e pacotes correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos e pacotes correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem

TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos e pacotes correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

1.5.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

ANEXO 04 DO TERMO DE REFERENCIA

1. SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

1.1. Tem por objetivo identificar, analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados descobriu-se que de fato eram um ataque iminente ao CONTRATANTE, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um CSOC do inglês *Cyber Security Operations Center*, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e às boas práticas de mercado já conhecidas.

Serviços de Resposta a Incidentes de Segurança		
Grupo de Serviço	**ID**	**Serviço**
Resposta a Incidentes de Segurança	1	Identificação da Causa
	2	Tratamento da Causa
	3	Aplicação/Orientação da correção
	4	Validação do contorno do incidente
	5	Encerramento do registro do incidente

1.2. As equipes envolvidas devem interagir e funcionar de maneira integrada, ou seja, devem compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e devem possuir conhecimento das tácticas e técnicas de ataque para que, por meio da atuação conjunta, aumente-se a efetividade da proteção do ambiente.

1.3. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

1.3.1. Todas as ferramentas e soluções de software deverão possuir os seguintes requisitos nativos, a saber:

1.3.1.1. A CONTRATADA deverá utilizar ferramenta de orquestração e automação do processo de resposta à incidentes, visando a diminuição de erros operacionais e consistência de atendimento.

1.3.1.2. Permitir integração com qualquer sistema de correlação de eventos (SIEM) para recebimento de alertas e abertura automática de incidentes para tratamento via fluxo de trabalho. A plataforma contratada deverá suportar o recebimento de alertas em formato Syslog;

1.3.2. Alinhado a uma gestão eficiente do processo de resposta a incidentes, a CONTRATADA deve possuir uma solução de orquestração e automação de resposta a incidentes com o intuito de simplificar processos complexos, acelerar fluxos, reduzir a carga de trabalho e tornar a operação de Segurança Cibernética mais eficiente;

1.3.3. O SOAR deve ajudar a transformar tarefas manuais do time de segurança cibernética em um processo automatizado e eficiente otimizando várias etapas no fluxo de tratamento e respostas. Através de processos bem elaborados, enriquecimento de contexto e outros recursos de investigação, o SOAR deve ser capaz de ajudar as equipes de resposta a incidentes a qualificar, colaborar e gerenciar incidentes mais rapidamente;

1.3.4. As equipes de segurança em qualquer nível de maturidade operacional devem estar aptos a usar o SOAR. O time de segurança cibernética deverá responder com eficiência, lidar com casos de uso complexos e aumentar a maturidade da segurança;

1.3.5. Conforme o time de segurança cibernética torna-se mais eficiente, ele pode assumir casos de uso mais desafiadores. Com o SOAR processos com várias interações devem ser automatizadas usando processos padronizados de Playbooks.

1.4. **EQUIPE DE INTELIGÊNCIA DE AMEAÇAS**

1.4.1. A contratada deverá contar com uma equipe de Inteligência de ameaças, dedicada a identificar as intenções, capacidades e, prioritariamente, as oportunidades usadas pelos criminosos através da coleta, normalização, correlação e análise de dados, transformando-os em inteligência e entregando ao CONTRATANTE relatórios periódicos, apresentando dados de mercado e o atual cenário do ambiente do CLIENTE.

1.4.2. Esses dados poderão ser utilizados para melhora na proteção, seja na atuação direta com a equipe de Hunting em novos casos de uso ou mantendo os times da CONTRATANTE informados, através de Boletins de Ameaças.

1.4.3. A CONTRATADA deverá possuir célula que entregue informações através de fontes de inteligências abertas e/ou próprias, compartilhando informações de inteligência através do MISP (Malware Information Sharing Platform), executando também a gestão através da equipe local, bem gerindo a integração entre o MISP da CONTRATANTE com o da CONTRATADA.

1.4.4. A Plataforma deverá ter capacidade de identificar vulnerabilidades em no máximo um dia após o surgimento desta, executar o correlacionamento com o inventário informado pela CONTRATADA e informar via evento no MISP sobre os sistemas vulneráveis.

1.4.5. A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de comprometimento) contendo, no mínimo,

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

hashes de binários maliciosos nos formatos MD5, SHA1, SHA256, *filename*, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;

1.4.6. Deve possuir equipe de *Threat Intelligence* que execute Análise de Superfície, um trabalho que avalia o ambiente na perspectiva de um agente malicioso em busca de eventuais brechas utilizando o framework OSINT (Inteligência de Fontes Abertas) com foco na identificação de superfície de ataque e as possíveis oportunidades na perspectiva de um agente malicioso.

1.4.7. Deve executar de forma recorrente a Análise de Superfície, no mínimo trimestralmente, utilizando especialistas de *Cyber Threat Intelligence* na execução de um assessment interno e análise externa utilizando técnicas de OSINT, apresentando informações dos perímetros com objetivo de entregar relatório, apontando de forma prática como tratar cada ponto identificado e apresentar um score qualitativo de maturidade para o CONTRATANTE.

1.5. **PROCESSO DE CAÇADA CONTINUA A AMEAÇAS**

1.5.1. Com o aumento do volume e complexidade das ameaças será exigido que a empresa CONTRATADA execute processos manuais de caçada de ameaças (threat hunting) semanalmente no ambiente da FUNPRESP.

1.5.2. A fim de balizar todo o processo de caçada de ameaças, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir IPSIS LITERIS.

1.5.3. A CONTRATADA deverá inclusive nos finais de semana e feriados, a:

1.5.3.1. Definir uma hipótese e uma declaração de uma possibilidade de ameaça, tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;

1.5.3.2. Uma vez que a hipótese tenha sido definida a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.5.3.3. Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;

1.5.3.4. Caso sejam encontrados eventos maliciosos, estes entram no processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;

1.5.3.5. Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;

1.5.3.6. Todo processo deve ser documentado através da plataforma de gerenciamento de chamados, incluindo qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;

1.6. PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO.

1.6.1. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Assim, o início do processo de resposta a incidente de segurança se dará sempre que um evento adverso for submetido pelo **SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS** descrito no Anexo 03 do presente termo de referência, porém não se limitando a este. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.

1.6.2. A fim de balizar todo o processo de resposta a incidente de segurança do CONTRATANTE, e influenciado pelos principais *frameworks* de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.

1.6.3. O processo de resposta a incidente de segurança é iniciado assim que o grupo de triagem de eventos realizar a abertura de incidente de segurança na ferramenta descrita no tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS.

1.6.4. Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

1.6.5. Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

1.6.6. Como próximo passo, o grupo de resposta a incidente de segurança da CONTRATADA deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

1.6.7. Juntamente com o CONTRATANTE, o grupo de resposta a incidente de segurança da CONTRATADA deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente. Mais detalhes sobre definição da severidade se encontram no tópico NÍVEIS MÍNIMOS DE SERVIÇO.

1.6.8. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (*malware*).

1.6.9. Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

1.6.10. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança da CONTRATADA deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

1.6.11. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA, através do grupo de resposta a incidente de segurança inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.6.12. Inicia-se então o processo de restauração dos serviços e soluções afetadas. Todo este processo é de responsabilidade da CONTRATADA, sendo realizado pelo grupo de resposta a incidente de segurança da CONTRATADA.

1.6.13. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto um laudo sobre o incidente de segurança em questão.

1.6.14. Caso seja necessário a reconstrução do ataque, este deve ser realizado pela CONTRATADA em ambiente controlado, usando-se por exemplo de *sandbox* (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da CONTRATADA.

1.6.15. O grupo de resposta a incidente de segurança da CONTRATADA deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

1.7. ENTREGAS A SEREM REALIZADAS

1.7.1. Plano de Resposta a Incidentes COMPLETO contendo tratativas, quando couber, envolvidos, plano de comunicação, etc.;

1.7.2. Análise de Superfície baseada em Mitre Att&ck;

1.7.3. Relatório de cobertura de defesas (GAPs) com riscos e pontos vulneráveis

1.7.4. Classificação de alertas pelo Framework MITRE ATT&CK contendo:

1.7.4.1. Relatório de GAPs

1.7.4.2. Infográfico de Maturidade

1.7.4.3. Artefatos de Avaliação

1.7.4.4. Avaliação das Técnicas e Sub Técnicas

1.7.4.5. Matriz de Priorização

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.5. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de incidentes que resultaram em comprometimento da segurança	Soma de incidentes abertos que resultaram em comprometimento da segurança	Incidentes com comprometimento	Incidentes com comprometimento	Número total de incidentes com comprometimento
Quantitativo de incidentes que tenham potencial de comprometer a segurança	Soma de incidentes que tenham potencial de comprometer a segurança	Incidentes com potencial	Incidentes com potencial	Número total de incidentes com potencial
Quantitativo de incidentes que não tenham potencial de comprometer a segurança	Soma de incidentes que não tenham potencial de comprometer a segurança	Incidentes sem potencial	Incidentes sem potencial	Número total de Incidentes sem potencial
TOP 10 – IP de destino de incidentes de segurança	Soma do número de incidentes por IP de destino	Incidentes abertos/tratados por IP de destino	IP de destino	TOP do número de incidentes por IP de destino
TOP 10 – Incidentes de segurança por origem	Soma do número de incidentes por origem	Incidentes abertos/tratados por origem	Origem	TOP do número de incidentes por origem interna ou externa
TOP 10 – Tipos de Incidentes	Soma do número de incidentes por tipo	Incidentes abertos/tratados por tipo	Tipo	TOP 10 por tipo de incidente

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.7.6. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

ANEXO 05 DO TERMO DE REFERENCIA

1. SERVIÇO DE PROTEÇÃO DE TRÁFEGO DE BORDA

1.1. A CONTRATADA deverá fornecer durante toda a vigência do contrato dois equipamentos de firewall NGFW de perímetro, junto com todo o serviço aqui descrito, que suporte as demandas atuais e futuras da organização, possibilitando o crescimento e amadurecimento tecnológico da CONTRATANTE

2. DAS FERRAMENTAS A SEREM UTILIZADAS

2.1. FIREWALL DE NOVA GERAÇÃO

2.1.1. CARACTERÍSTICAS DE HARDWARE DO SERVIÇO

2.1.1.1. Todos os componentes ofertados no serviço devem ser novos, sem uso anterior e, estar em linha de produção e comercialização pelo fabricante dos mesmos no momento da proposta, não devendo haver anúncio de "fim de produção" (EOL - End-of-Life) nem de apresentação do fim de comercialização (EOS - End-of-Sale) até esta data.

2.1.1.2. Todos os componentes listados devem estar 100% disponíveis durante o serviço.

2.1.1.3. O serviço deve consistir em proteção de rede baseada em hardware dedicado, em um equipamento do tipo "appliance", possuindo sistema operacional próprio para a execução das funções especificadas. Não será aceito equipamento do tipo PC (Personal Computer) ou Servidor, com sistema operacional de uso genérico, adaptado para a função aqui especificada.

2.1.1.4. Deve fornecer funcionalidade SD-WAN, podendo este item ser composto por outros players, desde que possua certificação terceira NSS Labs.

2.1.1.5. Deve possuir 1 (uma) interface para console de acesso ao equipamento com conector RJ-45, USB e/ou serial.

2.1.1.6. Deve operar na faixa de temperatura de 0 a 40°C e, humidade relativa entre 10 e 90%.

2.1.1.7. Firewall baseado em appliance com funcionalidades de Next Generation Firewall (NGFW);

2.1.1.8. Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada;

2.1.1.9. Suporte a, no mínimo, 1.500.000 conexões simultâneas;

2.1.1.10. Suporte a, no mínimo, 55.000 novas conexões por segundo;

2.1.1.11. Throughput de, no mínimo, 11 Gbps de VPN IPSec;

2.1.1.12. Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to Site simultâneos;

2.1.1.13. Estar licenciado para, ou suportar sem o uso de licença, 15.000 túneis de clientes VPN IPSEC simultâneos;

2.1.1.14. Throughput de, no mínimo, 1 Gbps de VPN SSL;

2.1.1.15. Suporte a, no mínimo, 500 clientes de VPN SSL simultâneos;

2.1.1.16. Suportar no mínimo 2.5Gbps de Throughput de IPS;
2.1.1.17. Suportar no mínimo 1 Gbps de Throughput de Inspeção SSL;
2.1.1.18. Suportar no mínimo 2.1 Gbps de throughput de Controle de Aplicação;
2.1.1.19. Suportar no mínimo 1.6 Gbps de throughput de NGFW;
2.1.1.20. Suportar no mínimo 1 Gbps de throughput de Threat Protection;
2.1.1.21. Permitir gerenciar ao menos 64 Access Points;
2.1.1.22. Possuir ao menos 16 interfaces 1Gbps Gigabit Ethernet do tipo RJ45;
2.1.1.23. Possuir ao menos 02 interfaces 10 Gbps Gigabit Ethernet do tipo SFP+;
2.1.1.24. Possuir ao menos 08 interfaces 1Gbps Gigabit Ethernet do tipo SFP;
2.1.1.25. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
2.1.1.26. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
2.1.1.27. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
2.1.1.28. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris ou GNU/Linux;
2.1.1.29. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
2.1.1.30. As funcionalidades de proteção de rede que compõe a plataforma de segurança,
2.1.1.31. podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
2.1.1.32. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
2.1.1.33. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
2.1.1.34. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
2.1.1.35. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
2.1.1.36. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
2.1.1.37. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
2.1.1.38. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.1.1.39. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
2.1.1.40. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
2.1.1.41. Os dispositivos de proteção de rede devem suportar sFlow;
2.1.1.42. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

2.1.1.43. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
2.1.1.44. Deve suportar NAT dinâmico (Many-to-1);
2.1.1.45. Deve suportar NAT dinâmico (Many-to-Many);
2.1.1.46. Deve suportar NAT estático (1-to-1);
2.1.1.47. Deve suportar NAT estático (Many-to-Many);
2.1.1.48. Deve suportar NAT estático bidirecional 1-to-1;
2.1.1.49. Deve suportar Tradução de porta (PAT);
2.1.1.50. Deve suportar NAT de Origem;
2.1.1.51. Deve suportar NAT de Destino;
2.1.1.52. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
2.1.1.53. Deve poder combinar NAT de origem e NAT de destino na mesma política;
2.1.1.54. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.1.1.55. Deve suportar NAT64 e NAT46;
2.1.1.56. Deve implementar o protocolo ECMP;
2.1.1.57. Deve suportar SD-WAN de forma nativa;
2.1.1.58. Deve implementar balanceamento de link por hash do IP de origem;
2.1.1.59. Deve implementar balanceamento de link por hash do IP de origem e destino;
2.1.1.60. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
2.1.1.61. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
2.1.1.62. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
2.1.1.63. Enviar log para sistemas de monitoração externos, simultaneamente;
2.1.1.64. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.1.1.65. Proteção anti-spoofing;
2.1.1.66. Implementar otimização do tráfego entre dois equipamentos;
2.1.1.67. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.1.1.68. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.1.1.69. Suportar OSPF graceful restart;
2.1.1.70. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
2.1.1.71. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
2.1.1.72. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
2.1.1.73. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.1.1.74. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
2.1.1.75. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
2.1.1.76. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
2.1.1.77. A configuração em alta disponibilidade deve sincronizar: Sessões;
2.1.1.78. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
2.1.1.79. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
2.1.1.80. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
2.1.1.81. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
2.1.1.82. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;
2.1.1.83. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
2.1.1.84. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
2.1.1.85. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
2.1.1.86. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
2.1.1.87. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede;
2.1.1.88. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
2.1.1.89. Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW;
2.1.1.90. A console de administração deve suportar no mínimo inglês, Espanhol e Português;
2.1.1.91. A console deve suportar a administração de switches e pontos de acesso para melhorar o nível de segurança;
2.1.1.92. A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas;
2.1.1.93. Deverá suportar controles por zona de segurança;

2.1.1.94. Controles de políticas por porta e protocolo;
2.1.1.95. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
2.1.1.96. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
2.1.1.97. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e
2.1.1.98. Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
2.1.1.99. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
2.1.1.100. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
2.1.1.101. Deve suportar o protocolo padrão da indústria VXLAN;
2.1.1.102. A solução deve permitir a implementação sem assistência de SD-WAN;
2.1.1.103. Em SD-WAN deve suportar QoS, modelamento de tráfego, rotas por políticas, VPN IPSec;
2.1.1.104. A solução deve suportar a integração nativa com soluções de sandboxing, proteção de correio eletrônico, cache e firewall de aplicação Web;
2.1.1.105. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
2.1.1.106. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email;
2.1.1.107. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, WhatsApp, 4shared, Dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, googledocs.;
2.1.1.108. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
2.1.1.109. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
2.1.1.110. Identificar o uso de táticas evasivas via comunicações criptografadas;
2.1.1.111. Atualizar a base de assinaturas de aplicações automaticamente;
2.1.1.112. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
2.1.1.113. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

2.1.1.114. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
2.1.1.115. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule etc.) possuindo granularidade de controle/políticas para os mesmos;
2.1.1.116. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
2.1.1.117. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
2.1.1.118. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate etc.) possuindo granularidade de controle/políticas para os mesmos;
2.1.1.119. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
2.1.1.120. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
2.1.1.121. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
2.1.1.122. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;
2.1.1.123. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
2.1.1.124. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e AntiSpyware);
2.1.1.125. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
2.1.1.126. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
2.1.1.127. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
2.1.1.128. Deve permitir o bloqueio de vulnerabilidades;
2.1.1.129. Deve incluir proteção contra ataques de negação de serviços;
2.1.1.130. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;
2.1.1.131. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
2.1.1.132. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
2.1.1.133. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

de TCP;

2.1.1.134. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;
2.1.1.135. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
2.1.1.136. Detectar e bloquear a origem de portscans;
2.1.1.137. Bloquear ataques efetuados por worms conhecidos;
2.1.1.138. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
2.1.1.139. Possuir assinaturas para bloqueio de ataques de buffer overflow;
2.1.1.140. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
2.1.1.141. Identificar e bloquear comunicação com botnets;
2.1.1.142. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
2.1.1.143. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
2.1.1.144. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
2.1.1.145. Os eventos devem identificar o país de onde partiu a ameaça;
2.1.1.146. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
2.1.1.147. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
2.1.1.148. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
2.1.1.149. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
2.1.1.150. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
2.1.1.151. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
2.1.1.152. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
2.1.1.153. Possuir pelo menos 60 categorias de URLs;
2.1.1.154. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
2.1.1.155. Permitir a customização de página de bloqueio;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

2.1.1.156. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
2.1.1.157. Além do Explicit Web Proxy, suportar proxy Web transparente;
2.1.1.158. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
2.1.1.159. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
2.1.1.160. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
2.1.1.161. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
2.1.1.162. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
2.1.1.163. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
2.1.1.164. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
2.1.1.165. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
2.1.1.166. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;
2.1.1.167. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;
2.1.1.168. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

2.1.1.169. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
2.1.1.170. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
2.1.1.171. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
2.1.1.172. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
2.1.1.173. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
2.1.1.174. O QoS deve possibilitar a definição de tráfego com banda garantida;
2.1.1.175. O QoS deve possibilitar a definição de tráfego com banda máxima;
2.1.1.176. O QoS deve possibilitar a definição de fila de prioridade;
2.1.1.177. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
2.1.1.178. Suportar modificação de valores DSCP para o Diffserv;
2.1.1.179. Suportar priorização de tráfego usando informação de Type of Service;
2.1.1.180. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
2.1.1.181. Permitir a criação de filtros para arquivos e dados pré-definidos;
2.1.1.182. Os arquivos devem ser identificados por extensão e tipo;
2.1.1.183. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
2.1.1.184. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
2.1.1.185. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
2.1.1.186. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
2.1.1.187. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;
2.1.1.188. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
2.1.1.189. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
2.1.1.190. Suportar VPN Site-to-Site e Cliente-To-Site;
2.1.1.191. Suportar IPSec VPN;
2.1.1.192. Suportar SSL VPN;
2.1.1.193. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
2.1.1.194. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
2.1.1.195. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
2.1.1.196. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
2.1.1.197. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
2.1.1.198. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

2.1.1.199. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
2.1.1.200. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
2.1.1.201. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
2.1.1.202. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
2.1.1.203. Deverá manter uma conexão segura com o portal durante a sessão;
2.1.1.204. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
2.1.1.205. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
2.1.1.206. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
2.1.1.207. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
2.1.1.208. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
2.1.1.209. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
2.1.1.210. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
2.1.1.211. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
2.1.1.212. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;
2.1.1.213. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
2.1.1.214. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
2.1.1.215. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;

2.1.1.216. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

2.1.1.217. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;

2.1.1.218. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.1.1.219. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;

2.1.1.220. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

2.1.1.221. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

2.1.1.222. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;

2.1.1.223. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

2.1.1.224. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

2.1.1.225. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.1.1.226. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.1.1.227. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

2.1.1.228. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

2.1.1.229. A solução deve implementar técnicas de Call Admission Control para limitar o

número de chamadas simultâneas;

2.1.1.230. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.1.1.231. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

2.1.1.232. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes;

2.1.1.233. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.1.1.234. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz; 2.219);

2.1.1.235. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

2.1.1.236. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

2.1.1.237. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;

2.1.1.238. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;

2.1.1.239. A base de reconhecimento de aplicações através de DPI deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;

2.1.1.240. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;

2.1.1.241. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;

2.1.1.242. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

2.1.1.243. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;

2.1.1.244. ASLEAP; Null Probe Response / Null SSID Probe Response;
2.1.1.245. Long Duration;
2.1.1.246. Ataques contra Wireless Bridges;
2.1.1.247. Weak WEP;
2.1.1.248. Invalid MAC OUI.
2.1.1.249. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigadospela infraestrutura através do envio de pacotes de deauthentication;
2.1.1.250. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
2.1.1.251. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
2.1.1.252. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
2.1.1.253. Deve implementar autenticação administrativa através do protocolo RADIUS;
2.1.1.254. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
2.1.1.255. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
2.1.1.256. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
2.1.1.257. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
2.1.1.258. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
2.1.1.259. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
2.1.1.260. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAPSIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
2.1.1.261. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal;
2.1.1.262. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
2.1.1.263. A solução deve permitir a hospedagem do cative portal na memória interna do controlador wireless;
2.1.1.264. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
2.1.1.265. A solução deve permitir a coleta de endereço de e-mail dos usuários como método

de autorização para ingresso à rede;

2.1.1.266. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

2.1.1.267. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna;

2.1.1.268. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

2.1.1.269. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;

2.1.1.270. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

2.1.1.271. Após a criação de um usuário visitante, a solução deve enviar as credenciais por email para o usuário cadastrado;

2.1.1.272. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;

2.1.1.273. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

2.1.1.274. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

2.1.1.275. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

2.1.1.276. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

2.1.1.277. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

2.1.1.278. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

2.1.1.279. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;

2.1.1.280. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

2.1.1.281. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

2.1.1.282. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;

2.1.1.283. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

2.1.1.284. A solução deve apresentar graficamente a topologia lógica da rede, representar os

elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

2.1.1.285. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

2.1.1.286. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

2.1.1.287. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

2.1.1.288. A solução deve possuir ferramentas de diagnósticos e debug;

2.1.1.289. A solução deve suportar comunicação com elementos externos através de APIs;

2.1.1.290. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

2.1.1.291. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;

2.1.1.292. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;

2.1.1.293. A solução SD-WAN deve suportar NAT em contexto de saída (NAT Outbound) para um pool de IPs públicos;

2.1.1.294. A solução dever ser capaz de prover função Zero Touch Provisioning;

2.1.1.295. A solução deve suportar ADVPN entre Ponto Central e Unidades Remotas;

2.1.1.296. A configuração VPN IPSec deverá oferecer suporte para versão IKE v2.0;

2.1.1.297. A configuração VPN IPSec deverá oferecer suporte para DH Group 14 e 15;

2.1.1.298. A solução deve suportar aos seguintes protocolos: IPv6, VRRP ou Equivalente, VRF, BGP, OSPF, RIPv2, 802.1Q, BFD, Dynamic Multipath, Policy Based Routing,

2.1.1.299. Reconhecimento em camada 7 totalmente segregado da camada 4;

2.1.1.300. Deve, de forma alternativa, contar com um banco de dados interno, onde seja possível atrelar uma aplicação a um determinado IP ou range de IPs de destino;

2.1.1.301. O reconhecimento de aplicações, deve ser atualizado de forma dinâmica e totalmente transparente para o dispositivo;

2.1.1.302. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

2.1.1.303. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de, pelo menos, mais de 1.000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, entre outros);

2.1.1.304. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SDWAN em condições onde a largura de banda é modificada;

2.1.1.305. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e packet loss, onde seja possível configurar um valor de theshold para cada um destes itens, onde será utilizado como fator de decisão nas egras de SD-WAN;

2.1.1.306. A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links;
2.1.1.307. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
2.1.1.308. A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento;
2.1.1.309. A solução deve possibilitar a distribuição de peso em cada um dos links que compõe o SDWAN, a critério do usuário, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em: Número de Sessões. Volume de Tráfego. IP de Origem e Destino. Transbordo de Link (Spillover);
2.1.1.310. A Alta Disponibilidade provida pela solução de SD-WAN, independente em suas modalidades físicas ou virtual, deverá obedecer aos seguintes critérios: Suportar Balanceamento Ativo, Suportar Balanceamento Ativo Passivo, Suportar Balanceamento de até 4 peers;
2.1.1.311. A solução SD-WAN deve oferecer troubleshooting em console de linha de comando ou gráfica, onde seja possível: executar Packet Sniffer do tráfego interessante, filtrando por: IP e Porta, realizar debug detalhado das fases de negociação VPN;
2.1.1.312. A solução SD-WAN deve suportar marcação de pacotes DSCP nas definições e regras para tráfego

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 06 DO TERMO DE REFERENCIA

1. SERVIÇO DE INTELIGÊNCIA APLICADO À SEGURANÇA

1.1. Visa o monitoramento contínuo e ininterrupto de ameaças cibernéticas acessíveis na internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS e páginas de comércio eletrônico, identificando e reconhecendo os eventos de segurança da informação, aos quais devem ser analisados e processados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

1.2. O Serviço de Inteligência Aplicada à Segurança Cibernética poderá ser provido por meio de plataforma SaaS (software as a service) ou on-premises.

1.3. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento de riscos digitais que atendam o descritivo técnico a seguir;

1.4. Deverá identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis;

1.5. Coletar diariamente informações das principais fontes relevantes de inteligência, tais como: redes sociais, buscadores, deep web e páginas web, etc. sobre ameaças disponíveis pelo mundo, de categorias como phishing, código, propriedade intelectual, chaves/senhas, botnets, internet profunda (deep web), spam, aplicativos falsos e documentos confidenciais;

1.6. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças;

1.7. Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente da FUNPRESP-EXE em questão, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança;

1.8. Deverá permitir o gerenciamento, configuração e utilização centralizada de todos os recursos disponibilizados;

1.9. Deverá possuir painel de visualização de fácil utilização e configuração, permitindo a seleção da(s) funcionalidade(s) que será(ão) utilizada(s);

1.10. Deverá possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas;

1.11. Deverá ser possível, de forma simples e rápida, a alteração dos critérios de busca de informações de acordo com as necessidades da FUNPRESP-EXE;

1.12. Deverá fornecer análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo:

1.13. Visualização de perfis relacionados a palavras-chaves;

1.14. Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;

1.15. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas;

1.16. Apresentação dos dados filtrados em painéis com as principais fontes identificadas na busca.

1.17. Possibilitar a exportação das informações identificadas nos formatos CSV, JSON, bem como a geração de relatórios em PDF;

1.18. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;

1.19. A integração deve ser realizada por meio de API Rest;

1.20. Deverá identificar a emissão de certificados para domínios monitorados e de nomes similares a termos ligados à FUNPRESP-EXE;

1.21. Deverá identificar a criação de domínios monitorados e de nomes similares a termos pré-definidos e configuráveis;

1.22. Realizar o monitoramento de marcas, por palavras-chave definidas, na internet;

1.23. A solução deverá ser capaz de analisar imagens para identificar abuso de marca, a partir de modelos fornecidos pela FUNPRESP-EXE;

1.24. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas;

1.25. O serviço deverá realizar a detecção de domínios registrados que possam oferecer, no mínimo:

1.25.1. Riscos de serem utilizados de forma maliciosa, variações comuns de nome, permutações de caracteres e outros (typosquatng, nomes de domínios similares);

1.25.2. Descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual e seu conglomerado;

1.25.3. Capacidade de detecção de páginas de phishing por quaisquer meios disponíveis;

1.25.4. Validar domínios suspeitos em repositórios de phishing;

1.26. Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, IRC, Pastebin, Scribd, ReclameAQUI, Apple Store, 4Shared, Google Play, Vimeo e Github;

1.27. Deverá, previamente à contratação, possuir métodos de coleta de redes sociais, páginas, portais e fóruns na internet superficial, profunda e oculta ("clear web", "deep web" e "dark web");

1.28. Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc);

1.29. Realizar a análise de áudio de no mínimo 1 plataforma de mensagens, caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio;

1.30. Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pela FUNPRESP-EXE;

1.31. O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise;

1.32. Realizar análise de conteúdo de imagens (OCR);

1.33. Identificar, disponibilizar e possibilitar a análise de trechos anteriores e posteriores dos textos capturados, sendo possível identificar a origem e o desdobramento do(s) assunto(s) pesquisado(s), de acordo com as necessidades da FUNPRESP-EXE;

1.34. Atuar de forma efetiva, no mínimo, com os aplicativos WhatsApp, Telegram, Discord e IRC;

1.35. Possuir foco no Brasil com fontes relevantes relacionadas a grupos de fraudadores do sistema financeiro brasileiro;

1.36. Permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria;

1.37. Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta; Atuar de forma efetiva, no mínimo, com Twitter, Instagram, Youtube e Facebook;

1.38. Monitorar, no mínimo, a rede de compartilhamento de textos Pastebin e a plataforma de compartilhamento de códigos Github e Bitbucket;

1.39. A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados à FUNPRESP-EXE no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados;

1.40. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA;

1.41. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (servidores e colaboradores) da Funpresp-Exe em redes sociais;

1.42. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso da FUNPRESP-EXE ou que permitam burlar os meios de proteção desses direitos;

1.43. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque a reputação da instituição ou ainda a tentativa de captura de credenciais da FUNPRESP-EXE;

1.44. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube etc.) que tenham relação com a FUNPRESP-EXE e não seja autorizado por essa Fundação;

1.45. Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas;

1.46. Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas da FUNPRESP-EXE, divulgações relacionadas a clientes e empregados da FUNPRESP-EXE, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial;

1.47. A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura através do protocolo HTTPS;

1.48. A plataforma deve permitir realizar a abertura de chamados a partir de um evento;

1.49. A CONTRATADA deve possuir mecanismos próprios que realizem a monitoração das principais Redes Sociais (Facebook, Twitter, Linkedin, Instagram, YouTube, etc.) e lojas de aplicativos para Smartphones (Google Play Store e Apple Store);

1.50. A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, que verifique a utilização do uso indevido da marca do FUNPRESP-EXE no nome do domínio ou na URL cadastrada, contendo o domínio/URL cadastrado, a empresa que administra o registro do domínio, e os dados proprietário do domínio;

1.51. A CONTRATADA deverá acatar novas palavras-chave, listas de palavras, desde que estejam no contexto da mesma área de negócio da CONTRATANTE sempre que demandados pela FUNPRESP-EXE para elaboração dos parâmetros de busca a serem executados;

1.52. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência;

1.53. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências;

1.54. **PROCESSO DE ATENDIMENTO PARA INTELIGÊNCIA APLICADA A SEGURANÇA**

1.54.1. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;

1.54.2. A fim de balizar todo o processo de monitoramento de riscos digitais da FUNPRESP-EXE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris;

1.54.3. É sabido que para o sucesso de um monitoramento de riscos digitais, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição dos ativos digitais que deverão ser monitorados. Entenda-se por ativos digitais, marcas, domínios, aplicativos móveis e/ou usuários a serem monitorados;

1.54.4. Tal definição da relação de ativos digitais a ser monitorada, não deve ser tomada de forma unilateral pela CONTRATADA. A FUNPRESP-EXE deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base;

1.54.5. Espera-se que a relação de ativos digitais monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a relação de ativos digitais, para que em um cenário onde estes novos ataques sejam

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

direcionados à FUNPRESP-EXE, sejam detectados através dos serviços em questão;

1.54.6. O produto de um evento é a detecção de citações, termos ou referências aos ativos monitorados, seja na deep/dark web, na internet aberta, em páginas de compartilhamento, redes sociais e aplicativos monitorados, gerados pela solução de proteção de riscos digitais utilizada pela CONTRATADA para execução deste serviço. Uma vez definida a relação de ativos digitais monitorados, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta;

1.54.7. Caso a CONTRATADA identifique a ausência dos insumos (ativos) a ser gerado, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo, restaurando a monitoração do ativo;

1.54.8. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de riscos digitais da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

1.54.8.1. Eventos de Informação: Estes eventos não requerem qualquer ação. Este grupo de eventos deve ser utilizado quando há menção não criminosa a um ativo digital monitorado, por exemplo, uma menção simples em uma rede social contendo o nome da CONTRATANTE.

1.54.8.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento suspeito em relação a um ativo digital monitorado, por exemplo, uma menção na internet, deep ou dark web, ou qualquer outro meio monitorado, com contexto de ameaças e/ou ataques direcionados a CONTRATADA.

1.54.8.3. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Detecção de um vazamento de dados da CONTRATANTE e venda de informações em canais de fraude.

1.54.9. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

1.54.9.1. Para eventos do tipo informação, não é requerido qualquer tipo de ação, porém, os eventos devem ser armazenados durante a vigência do contrato.

1.54.9.2. Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, um analista que pertence ao grupo de

monitoramento de riscos digitais, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz.

1.54.9.3. Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no presente termo de referência.

1.54.10. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

1.54.11. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

1.54.12. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

1.55. ENTREGAS A SEREM REALIZADAS

1.55.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativa de Menções	Soma de menções detectadas	Menções detectadas	Menções detectadas	Número total de menções detectadas
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de takedown realizados	Soma de takedown realizados	Takedown solicitado	Takedown	Número total de Takedown realizados

1.55.2. Tais entregáveis, relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 07 DO TERMO DE REFERENCIA

1. SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

1.1. Este serviço tem o objetivo de conscientizar os usuários de tecnologia da CONTRATANTE sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificando proativamente os usuários que seriam vetores de ataques e tornando-os elegíveis para um programa de capacitação interna sobre boas práticas de segurança da informação no ambiente corporativo do CONTRATANTE e proativamente protegendo o ambiente do CONTRATANTE de forma eficiente contra e-mails e mensagens instantâneas contra vírus, spams, *phishing*, *botnets*, ameaças avançadas, vazamento de informações, entre outros.

Serviços de Conscientização de Segurança da Informação		
Grupo de Serviço	**ID**	**Serviço**
Conscientização de Segurança da Informação	1	Companha de Conscientização (Palestras)
	2	Informativo sobre resultado da Campanha de Conscientização
	3	Programa de capacitação interna sobre boas práticas de segurança da informação
	4	Campanha de Phishing Direcionado
	5	Informativo sobre resultado da Campanha de Conscientização de Phishing

1.2. O serviço dar-se-á em 3 (três) ciclos anuais, e tem como principais objetivos:

1.2.1. Criar, planejar e formalizar institucionalmente o Programa de Conscientização de Segurança da Informação da FUNPRESP-EXE;

1.2.2. Identificar o nível de maturidade atual do processo de conscientização em segurança da informação dos seus funcionários diretos e indiretos;

1.2.3. Definir o nível de maturidade desejado ao final do primeiro ciclo;

1.2.4. Definir a estratégia para se alcançar o nível de maturidade ao final do primeiro ciclo;

1.2.5. Definir governança e métricas para monitorar a efetividade do programa e suas ações de conscientização;

1.2.6. Executar ações previstas de conscientização em cada ciclo;

1.2.7. Criar proposta de ações de conscientização que serão executadas;

1.3. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

1.3.1. A CONTRATADA deverá suportar o serviço de conscientização de usuários com plataformas de simulação de phishing, envio de pesquisas de maturidade, divulgação de conteúdo e treinamento a distância.

1.3.2. As ferramentas deverão ser providas em formato SaaS ou similar, onde toda a responsabilidade de configuração e gestão ficará por conta da CONTRATADA.

1.3.3. O serviço deverá ter módulo específico para envio de simulações de ataques de phishing.

1.3.4. A CONTRATANTE deverá ter acesso, através de portal integrado, onde deverá ser possível acompanhar a eficiência e abrangência do programa.

1.3.5. A CONTRATANTE poderá sugerir alterações no portal, de forma a representar as necessidades da FUNPRESP-EXE.

1.3.6. Não serão aceitos qualquer software livre, OpenSource ou outros que não sejam do fabricante;

1.3.7. A Plataforma deve suportar no mínimo os seguintes idiomas, inglês, português Brasil e espanhol sendo que o conteúdo dos treinamentos deve ser provido também, nas mesmas línguas já citadas

1.3.8. Deve suportar integração com Azure Active Directory e LDAP Active Directory;

1.3.9. A solução deve ser provida 100% em nuvem e não deve ser exigir nenhum servidor adicional, IP dedicado para disparos de e-mail, tão pouco registro de domínios para a sua plena execução;

1.3.10. Deve prover os seguintes módulos/funcionalidades através da console:

1.3.10.1. Customização e Simulação de Phishing via e-mail;

1.3.10.2. Customização e Simulação de Phishing via USB;

1.3.10.3. Treinamentos;

1.3.10.4. Exames e Testes;

1.3.10.5. Relatórios e Indicadores

1.3.10.6. Materiais Adicionais como cartilhas, papel de paredes, vídeos etc.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.11. Treinamentos devem obrigatoriamente ser:

1.3.11.1. Vídeos, Gaming (jogos) e módulos Interativos;

1.3.11.2. Entre 5 min a 20 min cada treinamento;

1.3.11.3. Ser providos em inglês, português e espanhol;

1.3.11.4. Deve ser possível substituir logo da plataforma para logo corporativo da empresa

1.3.11.5. Caso não haja integração SAML, deve ser possível implementar políticas de senhas complexas;

1.3.11.6. A plataforma deve possuir a característica de repositório de imagens customizadas para serem utilizadas em simulações de phishing e treinamentos customizados;

1.3.12. A customização de novos templates de e-mail phishing deve possuir as seguintes características:

1.3.12.1. Lista de domínios próprios providos pelo fabricante da solução que podem ser utilizados nas simulações, sem qualquer ônus adicional para a sua utilização;

1.3.12.2. Devem possuir domínios para serem utilizados no conceito de "impersonation";

1.3.12.3. Deve possuir domínios parecidos com grandes marcas no mínimo, nos seguintes segmentos de negócios:

a) Financeiro, no mínimo domínios parecidos com a Paypal;

b) Corporativo, no mínimo domínios parecidos com Onedrive, Sharepoint, Outlook e HP;

c) Tecnologia, no mínimo domínios parecidos com Microsoft;

d) Redes Sociais, no mínimo domínios parecidos com LinkedIn;

e) Comercial, no mínimo domínios parecidos com Adobe;

f) Serviços de Cloud, no mínimo domínios parecidos com Dropbox;

g) Consumo final, no mínimo domínios parecidos com Gmail;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.13. A CONTRATADA deverá ter a possibilidade de personalização do portal, com alteração de identidade visual, criação de novos campos e criação de novos dashboard

1.3.14. O portal deverá apresentar uma visão geral do programa com dando visibilidade dos participantes das ações, sua área, cargo e localidades.

1.3.15. O portal deverá permitir a visualização dos resultados das campanhas considerando:

1.3.15.1. Número de e-mails de phising enviados

1.3.15.2. Taxa de envio de phising

1.3.15.3. Número de e-mails de phising abertos

1.3.15.4. Taxa de abertura de phising

1.3.15.5. Número de e-mails de phising clicados por usuários

1.3.15.6. Taxa de cliques em e-mails phising

1.3.15.7. Número de usuários que submeteram dados

1.3.15.8. Taxa de submissão de dados

1.3.16. O portal deverá apresentar minimamente os seguintes indicadores de público de risco:

1.3.16.1. Número total da Amostragem

1.3.16.2. Percentual de Usuários com alto grau de risco

1.3.16.3. Quantidade total de usuários com alto grau de risco

1.3.16.4. Percentual de usuários com reincidência em campanhas de phising

1.3.16.5. Quantidade total de usuários com reincidência em campanhas de phising

1.3.16.6. Indicadores de total de participantes da campanha por áreas

1.3.16.7. Indicadores de total de participantes da campanha por cargo

1.3.16.8. Indicadores de estratégia educativas de ataques adotadas

1.3.16.9. Sumário de acompanhamento da efetividade das ações com relacionando o usuário com a estratégia adotada e o status ações realizadas (submissão de dados ou link clicado).

1.3.17. O portal deve permitir a criação de filtros por estratégia adotada, por localidade, por área e por cargo;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.3.18. O serviço deverá apresentar, em portal web, uma análise cruzada, das informações de credenciais vazadas, frente aos usuários de maior risco identificados no programa de conscientização e frente aos usuários de maior risco identificado pelo serviço de monitoração de segurança.

1.3.19. A solução deve possuir no mínimo 80 campanhas prontas, destinadas ao público brasileiro, que despertem o interesse dos usuários com os temas iguais ou similares a:

1.3.19.1. Amazon Prime, Netflix ou similares;

1.3.19.2. Armazenamento em serviços de nuvem;

1.3.19.3. Ferramentas de comunicação;

1.3.19.4. Redes sociais;

1.3.19.5. Comunicações sobre serviços de rede;

1.3.19.6. Serviços financeiros;

1.3.19.7. Serviços Apple;

1.3.19.8. Comunicados de apelo social.

1.3.20. A solução deve possuir a capacidade de criação de campanhas personalizadas de e-mails de phishing;

1.4. CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

1.4.1. A CONTRATADA deverá prover mecanismo de conscientização de ataque *phishing* aos usuários que utilizam os sistemas do CONTRATANTE, com intuito de mitigar riscos aos principais sistemas de comunicações e educar usuários quanto as normas internas do CONTRATANTE e boas práticas de segurança da informação;

1.4.2. A solução deverá implementar módulo educacional de uso ilimitado durante o período do contrato para reconhecimento de ataques de *phishing*, contemplando todos os usuários do CONTRATANTE. Caso não exista este tipo de licenciamento deverão ser entregues no mínimo 250 possibilidades de utilização do módulo educacional para cada usuário do CONTRATANTE a serem utilizados a cada 12 meses, não cumulativos;

1.4.3. A solução deve implementar módulo educacional contra ataques de phishing desenhado especificamente para este fim, onde não serão aceitas simulações executadas a partir dos softwares que compõem a proteção do tráfego de e-mail do CONTRATANTE;

1.4.4. A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerando os recursos do CONTRATANTE para o envio dos e-mails de simulação;

1.4.5. A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos;

1.4.6. A solução deve implementar módulo educacional contra ataques de *phishing*, todos no mesmo software, composto de no mínimo, a saber:

1.4.6.1. Modulo de construção de e-mail para simulação do ataque de *phishing*;

1.4.6.2. Modulo de conscientização educacional de reconhecimento do ataque de *phishing*;

1.4.6.3. Módulo gráfico e de relatórios que permita avaliar se o usuário reportou à área de segurança o possível ataque de *phishing* sofrido;

1.4.7. A solução educacional contra ataques de *phishing* deve ser capaz de criar templates educacionais exclusivos para o CONTRATANTE, em português com a logo marca do CONTRATANTE;

1.4.8. A solução educacional contra ataques de *phishing* deve ser capaz de criar templates educacionais exclusivos para o CONTRATANTE, com departamentalização direcionada por setor do CONTRATANTE como por exemplo, área administrativa, área jurídica, área técnica de TI, área técnica administrativa, não se limitando somente à estas áreas, em português e com a logo marca do CONTRATANTE;

1.4.9. A solução educacional contra ataques de *phishing* deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas ou externas à solução;

1.4.10. A solução educacional contra ataques de *phishing* deve ser capaz de, durante a criação do e-mail template customizado para o CONTRATANTE, conter no mínimo as parametrizações abaixo:

1.4.11. Escolha de um anexo customizado pelo CONTRATANTE a ser anexado ao e-mail de simulação de ataque *phishing*; seleção de usuário e de grupo de usuários que farão parte da simulação;

1.4.12. Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, específica por grupo a ser atingido;

1.4.13. Definição de assunto do e-mail de simulação do ataque *phishing*;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.4.14. Definição do nome do remetente que enviará o e-mail de simulação do ataque *phishing*;

1.4.15. Definição do endereço (usuário e domínio) do e-mail de simulação do ataque *phishing*.

1.4.16. A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:

1.4.16.1. Nome do usuário;

1.4.16.2. Sobrenome;

1.4.16.3. Endereço de e-mail;

1.4.16.4. Nome da empresa;

1.4.16.5. Dia / Data / Hora / Ano.

1.4.17. A solução educacional contra ataques de *phishing* deve ser capaz de criar relatórios executivos e mostrar de forma gráfica no console do produto no mínimo:

1.4.17.1. Verificação de quantas simulações foram enviadas para o CONTRATANTE;

1.4.17.2. Verificação de quantos usuários acessaram o e-mail de simulação de ataque *phishing*;

1.4.17.3. Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque *phishing*;

1.4.17.4. Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque *phishing*;

1.4.17.5. Verificação de quantos usuários reportaram para a área de TI a existência de um ataque *phishing*;

1.4.17.6. Verificação de quantos usuários executaram o módulo de conscientização educacional antiphishing;

1.4.17.7. Verificação da geolocalização dos usuários que sofreram a simulação do ataque de *phishing* e foram capturados na simulação.

1.4.18. A solução educacional contra ataques de *phishing* deve ser capaz de construir uma mensagem de conscientização direcionada para cada departamento informando que usuário foi pego em uma simulação de ataque *phishing*, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.4.19. A solução educacional contra ataques de *phishing* deve ser capaz de indicar a necessidade de o usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização (item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários;

1.4.20. A solução educacional contra ataques de *phishing* deve apresentar de forma gráfica o resultado geográfico de qual localidade o e-mail de simulação do ataque *phishing* foi efetivo com usuários sendo atacados pela simulação;

1.4.21. A solução educacional contra ataques de *phishing* deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização dos usuários da CONTRATANTE.

1.5. PROCESSO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

1.5.1. No intuito de balizar todo o processo de conscientização de segurança da informação do CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir.

1.5.2. O início do processo de conscientização de segurança da informação, dar-se-á através de uma reunião envolvendo o grupo de resposta a incidente da CONTRATADA e o time de segurança do CONTRATANTE. Esta reunião terá a seguinte pauta, a saber:

1.5.2.1. Definição do período de execução da campanha de conscientização.

1.5.2.2. Definição do tema do phishing controlado a ser enviados para os usuários.

1.5.2.3. Definição do grupo alvo do CONTRATANTE, que receberá o phishing controlado.

1.5.2.4. Definição do alcance, isso quer dizer, se a campanha apenas validará quais usuários receberam e clicaram no phishing controlado, ou também terá a possibilidade de captura dos dados dos usuários do grupo alvo.

1.5.3. Após o agendamento, será de responsabilidade da CONTRATADA a criação de um relatório de abertura de campanha, a qual documentará as

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

definições acordadas. Tal relatório deverá ser enviado para o time de segurança do CONTRATANTE, a qual terá a responsabilidade de aprovar a execução do serviço, conforme definições previstas em tal relatório.

1.5.4. Após a autorização do CONTRATANTE, a CONTRATADA terá a responsabilidade de iniciar a execução dos serviços, observando e seguindo as definições acordadas e autorizadas previamente.

1.5.5. Ao término da campanha será de responsabilidade da CONTRATADA, apresentar os resultados dos serviços, de tal forma que o CONTRATANTE consiga compreender:

1.5.5.1. Quais usuários clicaram no phishing, e informaram seus dados.

1.5.5.2. Quais usuários apenas clicaram no phishing.

1.5.5.3. Quais usuários apenas receberam o phishing e não clicaram.

1.5.6. Os usuários que clicaram e/ou informaram seus dados na campanha, serão elegíveis para um treinamento de segurança da informação para usuários finais, que deve abordar os temas que tem realização com a política de segurança da informação do CONTRATANTE.

1.5.7. A criação e aplicação deste treinamento será de responsabilidade da CONTRATADA. A modalidade dos treinamentos pode ser presencial, e/ou do tipo e-learning (modalidade de educação através da qual se faz necessário o uso de um ambiente virtual de aprendizagem).

1.5.8. Ao final de cada treinamento, os usuários necessariamente precisam ser avaliados, a fim de saber se o objetivo do treinamento foi alcançado. Tal avaliação também é de responsabilidade da CONTRATADA. Usuários que não alcançarem o mínimo necessário na avaliação, deverão passar pelo ciclo de treinamento novamente.

1.5.9. A definição de execução dos treinamentos pelos funcionários elegíveis é de responsabilidade do CONTRATANTE, cabendo a CONTRATADA ter o ambiente preparado sempre que solicitado pelo CONTRATANTE.

1.6. ENTREGAS A SEREM REALIZADAS

1.6.1. Para acompanhamento do serviço a ser ofertado pela CONTRATADA, os entregáveis abaixo deverão compor o relatório mensal a ser entregue pela CONTRATADA para acompanhamento da execução contratual;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.6.2. Relatório de Campanha Phishing deve conter, no mínimo, as seguintes informações:

1.6.3. ABA SUMÁRIO:

a) Status (Iniciada, em andamento, encerrada);

b) Data de criação;

c) Data de início;

d) Data de encerramento;

1.6.4. DETALHES DA CAMPANHA:

a) E-mail de Origem;

b) Assunto;

c) URL Phis;

d) URL do Aviso;

e) URL Cartilha;

f) Anexo(s);

g) Dados capturados (sim/não);

h) Dados Armazenados (sim/não);

i) Total de usuários alvos;

1.6.5. QUANTIDADE DE COLABORADORES POR TIPO DE EVENTO:

a) Abriram e-mail;

b) Clicaram no e-mail;

c) Submeteram dados;

d) Abriram a Cartilha;

1.6.6. ABA DETALHES DE ENVIO:

a) E-mail;

b) E-mail lido;

c) Clique em Link;

d) Submeteu Dados;

e) Cartilha Aberta;

f) O.S;

g) Browser;

1.6.7. ABA DETALHES DE USUÁRIOS:

a) Nome Completo;

b) Email;

c) Enviado em:

d) Visualizado em:

e) Clique no Link do E-mail;

f) Timestamp;

g) Endereço IP;

h) Location;

i) BrowserX - Operation System;

1.6.8. ESTATÍSTICAS:

a) Quantitativo de browsers baseados em User-Agents;

b) Quantitativo de sistemas operacionais baseados em User-Agents;

c) Quantitativo de localizações baseadas em User-Agents;

d) Lista de IPS por acesso;

e) Lista de IPS por localização;

ANEXO 08 DO TERMO DE REFERENCIA

1. SERVIÇOS TÉCNICOS ESPECIALIZADOS

1.1. Os Serviços Gerenciados de Segurança devem englobar a prestação de serviços técnicos evolutivos em segurança da informação, sob demanda.

1.2. Os serviços devem ser baseados em horas de serviço, envolvendo atividades a serem demandadas por meio de celebração prévia de solicitação formal de serviço, de comum acordo entre o CONTRATANTE e a CONTRATADA, cujo pagamento será efetivado após a entrega dos serviços e relatório de execução;

1.3. O pagamento será somente efetivado de acordo com a utilização da consultoria, o mês que não houver a prestação desse tipo de serviço por hora, o serviço não será faturado.

1.4. Os serviços técnicos especializados em segurança da informação devem atender os seguintes requisitos mínimos:

1.5. Execução de até 480 (quatrocentos e oitenta) horas/ano de serviço, sem garantia de execução em sua totalidade, tratando-se apenas de uma estimativa de execução de serviços no escopo da solução de Serviços Gerenciados de Segurança, limitando-se, exclusivamente, aos seguintes casos:

1.5.1. Elaboração de pareceres em segurança da informação;

1.5.2. Análise e suporte de planos de melhoria de infraestrutura e sistemas de segurança;

1.5.3. Suporte a mudanças de arquitetura do ambiente computacional;

1.5.4. Apoio na definição e implementação de mecanismos futuros de monitoramento e recursos de segurança;

1.5.5. Desenvolvimento e implantação de indicadores de segurança não previstos;

1.5.6. Orientação quanto ao procedimento de auditoria forense no ambiente computacional;

1.5.7. Transferência de conhecimento por meio de workshops para questões especificas aplicadas às atuais soluções implementadas.

1.5.8. Elaboração de estudos e documentações de segurança da informação;

1.5.9. Apoio na análise de riscos de segurança e na definição de controles e requisitos de segurança;

1.5.10. Apoio na elaboração e revisão de GAP analysis de políticas, normas, procedimentos e baselines de segurança;

1.5.11. Apoio em novas implementações e/ou suporte de soluções de segurança da informação;

1.5.12. Apoio em projetos de segurança da informação.

1.5.13. Execução de serviços por meio de Ordem de Serviço Técnico Especializado, previamente definida, documentada, protocolada e aprovada ao tempo necessário de atendimento;

1.5.14. Execução de serviços por meio de solicitação formal de Serviço Técnico Especializado, previamente definida, registrada e aprovada ao tempo necessário de atendimento;

1.5.15. Conclusão e validação de uma solicitação formal de Serviço Técnico Evolutivo somente após a entrega da documentação dos procedimentos.

1.6. SOLICITAÇÃO DOS SERVIÇOS TÉCNICOS

1.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA serão solicitados por meio de uma formalização utilizando-se de canais de comunicação oficiais usados na CONTRATANTE para controle das atividades a serem realizadas.

1.6.2. As solicitações deverão obrigatoriamente identificar:

1.6.2.1. Nome do responsável solicitante que deverá acompanhar a execução e declarar, no encerramento, a qualidade dos serviços prestados;

1.6.2.2. Objeto dos serviços: deverá ser descrito o escopo que o serviço pretende atender;

1.6.2.3. Descrição do processo de negócio, dos requisitos ou outros documentos complementares, onde serão especificadas as necessidades gerais a serem contempladas pelo projeto, e que possam ser úteis para que a CONTRATADA realize a especificação dos serviços;

1.6.2.4. Quantidade total de esforço estimado para conclusão dos serviços;

1.6.2.5. Cronograma físico-financeiro: planejamento da execução das atividades e os correspondentes desembolsos proporcionais que deverão ocorrer em um determinado período;

1.6.2.6. Data máxima para conclusão: determinar o prazo para que o serviço esteja concluído;

1.6.2.7. Artefatos/produtos a serem produzidos: definição do produto;

1.6.2.8. Descrição das tarefas: descrever as principais tarefas a serem realizadas;

1.6.2.9. Dados da autorização: nome/cargo/telefone do autorizador dos serviços, e data da autorização;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

1.6.2.10. Eventuais erros ou disfunções encontradas serão reportados oficialmente para a CONTRATADA, que deverá proceder as correções sem ônus para o CONTRATANTE.

1.6.2.11. Os produtos nos quais não forem detectados não conformidades, receberão o termo de aceite, documento necessário ao processo de pagamento do serviço.

1.6.2.12. O termo de aceite não exclui da CONTRATADA, a responsabilidade pelos erros não detectados, e nem a exime da responsabilidade sobre a qualidade, garantia e manutenção corretiva dos serviços.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 09 DO TERMO DE REFERENCIA

1. SERVIÇOS DE TESTES DE INVASÃO

1.1. Tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica da Fundação. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos de informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

1.2. Será executado 1 teste de invasão por mês, com abrangência estimada de até 50% dos serviços de TI do parque tecnológico.

1.3. Para a adequada prestação deste serviço a CONTRATADA deverá:

1.3.1. observar as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATANTE;

1.3.2. realizar testes de vulnerabilidades e invasão em endereços IP's, URL´s, aplicações ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao teste de invasão;

1.3.3. realizar os testes de invasão conforme a quantidade definida em Ordem de Serviço (OS);

1.3.4. os testes solicitados em Ordem de Serviço poderão ser do tipo White Box, Black Box ou Grey Box;

1.3.5. os testes poderão ser realizados a partir da rede interna da CONTRATANTE ou a partir da Internet, conforme solicitação da CONTRATANTE;

1.3.6. obedecer às premissas e condições das atividades de testes nos alvos definidos, de acordo com o estabelecido na respectiva Ordem de Serviço (OS);

1.3.7. reportar imediatamente quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo da Fundação, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

1.3.8. suspender imediatamente os testes sempre que uma indisponibilidade for causada em virtude da sua execução.

1.4. O teste de invasão deverá obedecer às seguintes fases:

1.4.1. Planejamento: todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento. Conterá informações sobre o ambiente corporativo,

utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):

1.4.1.1. Técnica Black Box (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista);

1.4.1.2. Técnica White Box (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste);

1.4.1.3. Técnica Grey Box (conhecimento limitado sobre o alvo).

1.4.2. Descoberta: deverão ser utilizadas, pelo menos, as ferramentas de análise de vulnerabilidades, descritas no objeto, gestão de vulnerabilidades, além de técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades. Nesta fase deverão ser atendidos os seguintes quesitos:

1.4.2.1. coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

a) Whois e nslookup (consultas DNS);
b) Sites de busca;
c) Listas de discussão;
d) Blogs de colaboradores;
e) Dumpster diving ou trashing;
f) Informações livres;
g) Packet sniffing “passive eavesdropping”;
h) Captura de banner.

1.4.2.2. coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

a) Port scanning (Mapeamento de rede);
b) Varredura de vulnerabilidade

i. a varredura de vulnerabilidade deverá verificar/identificar, entre outros:

- hosts ativos na rede;
- portas e serviços em execução;
- serviços ativos e vulneráveis nos hosts;
- sistemas operacionais;
- vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;
- configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
- identificação de vetores de ataque e cenários para exploração;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

- vulnerabilidades detectadas (CVE);
- vulnerabilidades de alto risco;
- vulnerabilidades de médio risco;
- vulnerabilidades de baixo risco;
- informações a serem aplicadas na fase de ataques.

ii. Dos serviços e aplicações web:

- uso indevido de sistema de arquivos e arquivos temporários;
- evasão de informação por configurações default de tratamento de erros;
- tratamento indevido de entrada;
- problemas relacionados à má configuração dos serviços;
- gerenciamento inseguro de sessões web.

1.4.3. Ataque (exploração):

1.4.3.1. deverão ser aplicados, no mínimo, os seguintes tipos de ataques:

a) violações do protocolo HTTP;
b) SQL injection;
c) LDAP injection;
d) cookie tampering;
e) cross-site scripting (XSS);
f) directory transversal;
g) buffer overflow;
h) OS command execution;
i) command injection;
j) remote code inclusion;
k) server side includes injection (SSI);
l) file disclosure;
m) information Leak;
n) zero day attacks;
o) DDos (distribuited denial of service);
p) Dos (denial of service) ;
q) contra protocolo TCP;
r) ataques contra a aplicação.

i. Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:

- bugs em serviços, aplicativos e sistemas operacionais;
- SYN flooding;
- fragmentação de pacotes de IP;
- smurf e fraggle;
- teardrop, nuke e land;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ii. Para ataques contra o protocolo TCP:
- sequestro de conexões;
- prognóstico de número de sequência do protocolo TCP;
- ataque de mitnick;
- source routing.

iii. Para ataques em nível da aplicação:
- buffer overflow;
- problemas com o SNMP;
- vírus, worms e cavalos de Tróia.

iv. Injeção de Código:
- ataques XSS (cross-site script);
- comprometimento do acesso remoto;
- manutenção de acesso;
- encobrimento de rastros da invasão.

1.5. Relatório de Teste de Invasão:

1.5.1. após a fase de ataque deverá ser elaborado e entregue à CONTRATANTE, o relatório "RELATÓRIO TESTE DE INVASÃO" para cada teste realizado, contemplando, no mínimo, as informações:

a) objetivos, premissas e escopo do teste;
b) datas e horas dos testes;
c) metodologia de análise de vulnerabilidades;
d) descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis;
e) recomendações e controles de segurança necessários para correção das vulnerabilidades
f) apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão;
g) detalhes da infraestrutura descoberta, alvo dos testes de invasão;
h) equipamentos e recursos demandados para este teste;
i) tipos de ataque;
j) prazos (janelas de tempo para execução dos testes);
k) pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes);
l) tipos de testes realizados pelos especialistas em segurança da informação;
m) confirmação ou refutação da existência de vulnerabilidades;

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

n) documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
o) obtenção de acesso e possível escalada de privilégios;
p) detalhamento da metodologia do ataque;
q) recomendações para sanar riscos e vulnerabilidades.

1.5.2. deverá ser realizada reunião para apresentação do relatório e descrição das atividades executadas durante o teste.

1.6. Relatório Final do Teste de Invasão

1.6.1. após a entrega do "RELATÓRIO DE TESTE DE INVASÃO", a Funpresp-Exe analisará o documento para aplicar as recomendações, remediar os riscos ou mesmo assumi-los.

1.6.2. após essa análise e aplicadas medidas de remediação, a Funpresp-Exe poderá solicitar que o teste de invasão seja refeito para aferição dos resultados com emissão de novo relatório.

1.6.3. o prazo para conclusão de cada Ordem de Serviço (OS), incluindo, diagnósticos, análises, avaliações e testes com fornecimento de todos os relatórios específicos de avaliação de vulnerabilidades, dos ambientes relacionados neste Termo de Referência, será definido de acordo com cada atividade, sendo divididas em:

a) atividades do Pentest;
b) entrega do relatório "Teste de Invasão";
c) ações corretivas das vulnerabilidades apontadas pela Contratada e aplicadas pela Funpresp-Exe;
d) reavaliação do Pentest, caso necessário;
e) entrega do relatório "Relatório Final do Teste de Invasão".

1.6.4. a Funpresp-Exe deverá aplicar, no que couber, correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório "Teste de Invasão" a partir do final da "reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste".

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 10 DO TERMO DE REFERENCIA

1. NÍVEIS MÍNIMOS DE SERVIÇOS

1.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após a mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

1.2. Para mensurar esses fatores são utilizados indicadores relacionados à natureza e característica do objeto da contratação, para os quais são estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA.

1.3. O não cumprimento dos valores mínimos/máximos exigidos nos indicadores ensejará em glosas de acordo com o estipulado nesta seção.

1.4. Os primeiros 90 (noventa) dias após o início da execução dos serviços serão considerados como período de estabilização, durante o qual os resultados esperados e os níveis de qualidade exigidos poderão ser implementados gradualmente, de modo a permitir à CONTRATADA realizar a adequação progressiva de seus serviços e alcançar, ao término desse período, o desempenho requerido.

1.5. Para os serviços previstos no Grupo 1, a apuração dos níveis de serviço será mensal e realizada do primeiro ao último dia do respectivo mês do faturamento e para os serviços previstos no Grupo 3, a apuração dos níveis de serviço será realizada após a conclusão de cada Ordem de Serviço.

1.6. Para cada inadimplemento, o CONTRATANTE aplicará glosa de 1% (um por cento) sobre o valor da nota fiscal a cada 20 pontos nas tabelas abaixo, limitada a glosa total ao percentual máximo de 30% (trinta por cento) do valor mensal previsto em contrato, devendo o CONTRATANTE cientificar à CONTRATADA sobre as razões que ensejaram o desconto. Ultrapassado este limite, a CONTRATADA fica sujeita à aplicação das penalidades descritas no Termo de Referência.

1.7. A apuração dos indicadores previstos nos serviços do Grupo 1 será realizada mensalmente a partir de Relatório Mensal de Acompanhamento, elaborado pela CONTRATADA, baseado no sistema de gerenciamento de chamados de TIC da CONTRATADA, além das demais ferramentas fornecidas no escopo desse contrato.

1.8. Para os indicadores previstos nos serviços do Grupo 3 ou para os quais não se mostrar possível o acompanhamento através dos softwares mencionados anteriormente, deverá ser utilizada uma planilha eletrônica para controle manual, elaborada pela CONTRATADA e validada pela Funpresp-Exe.

1.9. A Funpresp-Exe verificará a conformidade, por amostragem de dados, e solicitará os devidos ajustes nos casos de inconformidade. A CONTRATADA deverá realizar os ajustes em até 3 (três) dias corridos após a solicitação da Fundação.

1.10. O momento de início da medição do nível de serviço de cada atendimento/atividade solicitada à CONTRATADA será definido pela data e hora:

1.10.1. De designação do incidente, problema, tarefa de mudança ou requisição de serviço no Software de Gerenciamento de Serviços de TIC ou Incidentes de SI para a CONTRATADA; ou

1.10.2. De envio de e-mail pelo Gestor do Contrato ou equipe técnica da Funpresp-Exe; ou

1.10.3. De registro do evento na ferramenta de monitoração; ou

1.10.4. No caso dos serviços agendados, os tempos serão contados a partir do início da data e hora agendada para o referido atendimento.

1.11. A contagem do prazo para o atendimento poderá ser interrompida ou estendida com a anuência da Funpresp-Exe, desde que solicitada de forma justificada pela CONTRATADA antes do seu descumprimento.

1.12. No caso de discordância das glosas aplicadas, a CONTRATADA poderá apresentar recurso, que será analisado pela equipe de fiscalização. Se a decisão for favorável ao recurso da CONTRATADA, esta emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

1.13. O momento de fim da medição do nível de serviço de cada atendimento/atividade do Catálogo solicitada à CONTRATADA será definido pela data e hora da resposta da equipe da CONTRATADA pelo mesmo meio que foi registrado o atendimento.

1.14. A Funpresp-Exe analisará a corretude da resolução do atendimento para então aprovar ou recusar o fechamento dele. O tempo gasto pela Funpresp-Exe para analisar o atendimento será considerado para efeito de cálculo do tempo de resolução, caso a resolução seja recusada pela Funpresp-Exe.

1.15. Considerar-se-á como tempo de resolução, o período líquido compreendido entre o momento de início e a finalização do atendimento, descontado o tempo em que o mesmo ficou pendente de execução por outras equipes da Funpresp-Exe.

1.16. Para quaisquer indicadores de nível de serviço influenciados negativamente por eventos comprovadamente causados pela Funpresp-Exe não serão considerados os efeitos de tais eventos no cômputo do indicador de nível de serviço.

1.17. A tabela abaixo define os indicadores, níveis de serviço esperados e ajustes de pagamento para os serviços:

Grupo	Item	Indicadores de Nível de serviço	Cálculo com base no mês calendário	Meta exigida	Glosa por inadimplemento
1	1	Tempo máximo para resolução de requisições de serviços relacionadas aos Produtos de UTM	Tempo = Hora da resolução da solicitação – hora de início da solicitação	<= 90 minutos	10 pontos (+3 pontos a cada 30 minutos excedentes)
		Tempo máximo para resolução das demais requisições de serviços	Tempo = Hora da resolução da solicitação – hora da solicitação	<= 24 horas	10 pontos (+3 pontos a cada 6 horas excedentes)
		Tempo máximo para correção de incidente nos serviços de segurança da Funpresp-Exe, em caso de indisponibilidade	Tempo = Hora do restabelecimento – Hora do início da indisponibilidade	<= 120 minutos	30 pontos (+5 pontos a cada 30 minutos excedentes)
		Tempo máximo para abertura de chamados de suporte com terceiros	Tempo = Hora de abertura do chamado – hora da triagem	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedente)
	2	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente	<= 72 horas	5 pontos (+2 pontos a cada dia excedente)
	3	Tempo máximo para triagem de	Tempo = Hora da triagem –	<= 30 minutos	3 pontos (+1 ponto a cada 15

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

Grupo	Item	Indicadores de Nível de serviço	Cálculo com base no mês calendário	Meta exigida	Glosa por inadimplemento
		incidentes de segurança	Hora de entrada do evento de segurança		minutos excedentes)
		Tempo máximo para comunicação de incidentes a Central de Serviços da CONTRATADA e aos gestores de TI	Tempo = Hora da comunicação – hora da triagem	<= 30 minutos	5 pontos (+2 pontos a cada 15 minutos excedentes)
	4	Tempo máximo para resposta de incidentes de segurança de gravidade alta	Tempo = Hora do início da resposta – hora da triagem	<= 60 minutos	10 pontos (+3 pontos a cada 20 minutos excedentes)
		Tempo máximo para resposta de incidentes de segurança de gravidade média	Tempo = Hora do início da resposta – hora da triagem	<= 120 minutos	10 pontos (+3 pontos a cada 30 minutos excedentes)
		Tempo máximo para resposta de incidentes de segurança de gravidade baixa	Tempo = Hora do início da resposta – hora da triagem	<= 180 minutos	5 pontos (+2 pontos a cada hora excedente)
3	1	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço Exclusivas	Prazo Real – (Prazo Acordado + 25%)	<= 0	20 pontos

1.18. Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA:

Nº	Descrição	Referência	Glosa por inadimplemento
1	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária	Por profissional	30
2	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	50
3	Suspender, colocar como pendente, pausar ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	5
4	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável	Por regra incluída, alterada ou excluída	10
5	Fraudar, manipular ou descaracterizar indicadores, metas de níveis de serviço e de desempenho por quaisquer subterfúgios	Por ocorrência	100
6	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	200
7	Deixar de cumprir qualquer outra obrigação estabelecida no edital e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10
8	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada	Por ocorrência	5
9	Causar qualquer dano aos equipamentos do contratante por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50
10	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização.	Por ocorrência	10
11	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo CONTRATANTE.	Por ocorrência	10
12	Incluir, excluir ou alterar regras nos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	30
13	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada.	Por ocorrência	10
14	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique	Por ocorrência	30
15	Deixar de apresentar relatórios, levantamentos ou inventários no prazo determinado em comum acordo.	Por ocorrência	10

Nº	Descrição	Referência	Glosa por inadimplemento
16	Deixar de produzir ou de manter atualizadas as rotinas e scripts da Base de Dados de Conhecimentos.	Por ocorrência	5
17	Deixar de comunicar o contratante da substituição de profissionais responsáveis pela execução das atividades	Por ocorrência	10
18	Deixar de atuar tempestivamente no caso de incidentes graves	Por ocorrência	15
19	Deixar de documentar os ICs – Itens de Configuração e de manter completa e atualizada a Base de Dados de Configuração, inclusive no que diz respeito aos diagramas e desenhos, imediatamente após sua inclusão ou exclusão do ambiente.	Por ocorrência	2

1.19. Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA deixar de:

Nº	Descrição	Referência	Glosa por inadimplemento
1	Cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato	Por ocorrência	10 pontos
2	Cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pela Funpresp-Exe	Por ocorrência	15 pontos
3	Cumprir ou implementar as rotinas em conformidade com os processos de trabalho da Funpresp-Exe e da Gerência de Tecnologia da Informação (GETIC)	Por ocorrência	10 pontos
4	Elaborar auditorias de dados, consultas às bases de logs de transações ou relatórios diversos	Por ocorrência	15 pontos
5	Apresentar os relatórios consolidados conforme exigências do Termo de Referência até o dia 5º dia útil do mês subsequente	Por dia de atraso	5 pontos
6	Apresentar relatórios, levantamentos ou inventários conforme demanda em até 3 dias úteis	Por ocorrência	5 pontos
7	Apresentar mensalmente proposta de melhorias no ambiente	Por ocorrência	5 pontos
8	Notificar sobre ocorrências recorrentes	Por ocorrência	5 pontos
9	Manter o Configuration Management Database (CMDB) atualizado	Por ocorrência	10 pontos

Nº	Descrição	Referência	Glosa por inadimplemento
10	Manter a documentação e os desenhos das topologias atualizados e completos	Por ocorrência	5 pontos
11	Cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança	Por ocorrência	10 pontos
12	Analisar a viabilidade e o impacto da instalação de novas soluções ou correções	Por ocorrência	5 pontos
13	Deixar de notificar incidentes repetitivos, quer tenham sido conhecidos através do monitoramento ou por notificações de usuários, para a equipe segurança do CONTRATANTE.	Por ocorrência	5 pontos

1.20. Não serão considerados como Tempo de Indisponibilidade:

a) Falta de energia no local de prestação dos serviços;
b) Indisponibilidade da rede lógica do CONTRATANTE;
c) Problemas derivados de ocorrências no ambiente do CONTRATANTE, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
d) Ações necessárias para resolução de problemas que tenham sido autorizadas pelo CONTRATANTE;
e) Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos da Rede CONTRATANTE;
f) Indisponibilidade gerada pela necessidade de reparo ou troca dos equipamentos da solução de segurança da informação da rede CONTRATANTE, listadas do tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE) do presente termo de referência;
g) Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança do CONTRATANTE;
h) Indisponibilidade do ambiente virtualizado do CONTRATANTE, infraestrutura computacional em que parte dos softwares que compõe a solução deve ser instalada;
i) Manutenções programadas pelo CONTRATANTE;
j) Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pelo CONTRATANTE.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 11 DO TERMO DE REFERENCIA

1. CATÁLOGO DE SERVIÇOS

1.1. Este catálogo de serviços de apoio ao planejamento visa estabelecer e caracterizar grande parte dos serviços contemplados no objeto da contratação.

1.2. A estrutura deste catálogo é separada em quatro partes, de acordo com o tema da atividade:

1.2.1. Serviço de Operação e resposta a requisições

1.2.2. Serviço de Gestão de Vulnerabilidades

1.2.3. Serviço de Monitoramento de Ataques Cibernéticos

1.2.4. Serviço de Resposta a incidentes de segurança

1.3. Após o término da demanda, na fase de encerramento, a CONTRATADA poderá propor à Funpresp-Exe a atualização do catálogo. Se, por exemplo, uma determinada atividade vier a apresentar escopo maior do que o originalmente previsto no catálogo, esse processo permitirá medição mais precisa para demandas futuras. A FUNPRESP-EXE poderá, assim, alterar a dimensão do escopo de determinado item no catálogo, tanto por provocação da CONTRATADA, como por iniciativa própria. O catálogo só poderá ser atualizado antes do início do desenvolvimento de determinada demanda.

1.4. A seguir apresentamos os itens do catálogo de serviços.

1	**Serviço de Operação e Resposta a Requisições**		
	Grupo de Serviço	**ID**	**Serviço**
	Serviço de Operação e Resposta a Requisições	1	Fornecimento de ferramenta de proteção de endpoints
		2	Gerencia Centralizada dos clientes
		3	Instalação dos clientes via console
		4	Atualização de console
		5	Atualização dos Clientes via console
		6	Configuração de proteção endpoint
		7	Configuração de políticas de Firewall
		8	Configuração de Políticas de IPS
		9	Configuração de Políticas de Integridade do host
		10	Configuração de scans customizados
		11	Configuração de políticas de Controle de Aplicações e Dispositivos
		12	Criação de pacotes customizados para instalação do agente
		13	Configuração de Políticas de Grupo
		14	Configuração de integração (Servidores de Autenticação Suportados)
		15	Criação de Relatório de situação do parque (Atualização dos clientes)
		16	Configuração do método de autenticação de contas de administradores
		17	Configuração de política de segurança (L4/L7)
		18	Aplicação de política de Threat Prevention (antivírus, anti-spyware/bot ou IPS)
		19	Configurar integração com base de usuários (auth / AD)
		20	Aplicar controle de uso de aplicação por usuário/grupo de usuário
		21	Atualização firmware (SO)
		22	Criação de rota ou correção de tráfego assimétrico
		23	Configuração de PBF (Policy Based Forwarding)
		24	Aplicação de política de SSL Decryption
		25	Aplicação de categoria de URL filtering baseada em usuário/grupo de usuário
		26	Análise/criação de IOC (Indicator of Compromise)
		27	Criação de assinatura customizada para identificação e controle de aplicação
		28	Aplicação de políticas de QoS
		29	Health Check (relatório de adoção de uso de boas práticas de config)
2	**Serviço de Gestão de Vulnerabilidades**		
	Grupo de Serviço	**ID**	**Serviço**
	Serviço de Gestão de	1	Checagem (scan) e varredura em ativos de rede
		2	Checagem (scan) e varredura em aplicações web
		3	Análise de falso positivo em ativos de rede

	Vulnerabilidades	4	Análise de falso positivo em aplicações web
		5	Informativo sobre vulnerabilidades em ativos de rede
		6	Informativo sobre vulnerabilidades em aplicações web
		7	Suportar correções das vulnerabilidades em ativos de rede
		8	Suportar correções das vulnerabilidades em aplicações web
		9	Apresentar abordagem dinâmica para priorizar correções
3	**Serviço de Monitoramento de Ataques Cibernéticos**		
	Grupo de Serviço	**ID**	**Serviço**
	Serviço de Monitoramento de Ataques Cibernéticos	1	Eventos de Informação
		2	Eventos de Aviso
		3	Eventos de Exceção
4	**Serviço de Resposta a Incidentes de Segurança**		
	Grupo de Serviço	**ID**	**Serviço**
	Serviço de Resposta a Incidentes de Segurança	1	Identificação da Causa
		2	Tratamento da Causa
		3	Aplicação da correção
		4	Validação do contorno do incidente
		5	Encerramento do registro do incidente

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 12 DO TERMO DE REFERENCIA

1. DESCRIÇÃO DO AMBIENTE

1.1. REDE: 02 (DOIS) SEGMENTOS

1.1.1. Rede GPON.

1.1.2. Rede Gigabit Ethernet sobre par trançado.

1.2. INTERNET: 02 (DOIS) LINKS DE OPERADORAS DISTINTAS.

1.2.1. 500 Mbps.

1.2.2. 300 Mbps.

1.3. FIREWALL:

1.3.1. 02 (dois) EQUIPAMENTOS.

1.3.2. 03 (três) VPN.

1.4. HYPERVISOR:

1.4.1. 02 (dois) Microsoft Hyper-V.

1.5. SISTEMAS OPERACIONAIS:

1.5.1. Linux.

1.5.1.1. 13 (treze) Linux Debian

1.5.1.2. 2 (dois) Linux Ubuntu 22.04 LTS

1.5.1.3. 12 (onze) Linux Ubuntu 20.04 LTS

1.5.1.4. 01 (um) Linux Ubuntu 18.04 LTS

1.5.2. Windows.

1.5.2.1. 44 (quarenta e quatro) Windows 10

1.5.2.2. 215 (duzentos e quinze) Windows 11

1.5.2.3. 06 (seis) Windows Server 2012 R2

1.5.2.4. 25 (vinte e cinco) Windows Server 2019 Datacenter

1.5.2.5. 16 (dezesseis) Windows Server 2019 Standard

1.5.2.6. 02 (dois) Windows Server 2022 Datacenter

1.6. BANCOS DE DADOS:

1.6.1. 06 (seis) Sql Server.

1.6.2. 02 (dois) MySQL/MariaDB.

1.6.3. 02 (dois) PostgreSQL.

1.7. SERVIDORES WEB:

1.7.1. 2 Apache.

1.7.2. 8 Nginx.

1.7.3. 12 Internet Information Services

1.7.4. 08 (oito) Microsoft IIS.

1.8. WIFI: 04 (QUATRO) EQUIPAMENTOS:

1.8.1. 04(quatro) redes de acesso.

1.9. PROVEDOR DE CLOUD:

1.9.1. Amazon Web Service

1.10. SERVIÇOS:

1.10.1. 05 ACTIVE DIRECTORY

1.10.2. 01 AD CONNECTOR

1.10.3. 01 (um) BACKUP VEEAM

1.10.4. 02 (dois) DHCP

1.10.5. 04 (quatro) DNS

1.10.6. 04 (quatro) FILE SERVER

1.10.7. 01 (um) FTP

1.10.8. 01 (um) Servidor de IMPRESSÃO

1.10.9. 06 (seis) Clusters KUBERNETS

1.10.10. 602 (seiscentos e dois) POD (não conteiner)

1.10.11. 01 (um) O365 (480 caixas postais)

1.10.12. 02 (dois) SMTP

1.10.13. 01 (um) VAMT

1.10.14. 03 (três) VPN’s

1.10.15. 01 (um) VOIP

1.10.16. 03 (três) WEB SERVER

1.10.17. 01 (um) WSUS

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

2. AMBIENTE TECNOLOGICO

OBJETOS	QDE.
Appliance de Backup	01
Estações de Trabalho - Desktops	200
Estações de Trabalho - Notebooks	100
Firewalls	02
Nuvem AWS	01
Pontos de Acesso sem Fio	04
Servidores Físicos	08
Servidores Virtuais	100
Switch GPON	02
Switches	08
Telefonia IP	01
Usuários internos	500

TABELA 1 - CONJUNTO DE CONTROLES

3. PRINCIPAIS SERVIÇOS DE TI

3.1. A tabela a seguir apresenta os principais serviços de TIC da Funpresp-Exe, sendo a descrição desse quantitativo meramente descritiva, podendo ser alterada a qualquer instante sem a necessidade de divulgação prévia.

ID	SERVIÇO
1	Gerenciamento de logins, senhas e autenticação
2	Integração do AD Onpremisses com o Azure (Office365)
3	Gerenciamento de riscos
4	Aplicação autoserviço para troca de senha de usuários.
5	Base de conhecimento da GETIC
6	Sistema de Gerenciamento de banco de dados
7	Gerenciamento de servidores hardware
8	Gerenciamento de implantação de versões de sistemas
9	Repositório e versionador de código fonte
10	Integração contínua de código
11	Frontend de gerenciamento Kubernets

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – CONTRATANTE
SCN Quadra 2 Bloco A – Sala 202/ 203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

12	Gerenciamento de defeitos de software
13	Gerenciamento de binarios de sistemas
14	Frontend de gerenciamento Kubernets
15	Inspeção de qualidade de software
16	Gerenciamento de ativos de rede
17	Gerenciamento de máquinas virtuais
18	Registro de ligações
19	Solução de gestão previdenciária
20	Gerenciamento da Central Telefonica VOIP
21	Gerenciamento de inventario de hardware e software
22	Portal de gerenciamento de contas e recebimento e envio de e-mails
23	Software para gerenciamento de conexoes VPN
24	Software para gerenciamento de firewall de redes
25	Sistema de Perfis de Investimento
26	Divulgação de conteúdo institucional - interno
27	Divulgação de conteúdo institucional - externo
28	Gerenciamento de BI e Construção de paineis e dashboards
29	Gerenciamento de envio de emails de comunicação ao participante
30	Gestão de reuniões dos órgãos diretivos
31	Fornecimento de informações, extratos e serviços ao participante
32	Tramitação de processos eletrônicos
33	Gerenciamento de recebimento e envio de arquivos de forma segura
34	Gerenciamento de demandas de suporte técnico
35	Gerenciamento de investimentos
36	Gerenciamento de backups
37	Gerenciamento de backups de cluster Kubernetes
38	Monitoramento de ativos de TI

ANEXO 13 DO TERMO DE REFERENCIA

ORDEM DE SERVIÇO

1 – IDENTIFICAÇÃO			
Nº da OS		Data de emissão	
Contrato nº			
Objeto do Contrato			
Contratada		CNPJ	
Preposto			
Início vigência		Fim vigência	
ÁREA REQUISITANTE			
Unidade			
Solicitante		E-mail	

2 – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição do serviço	Métrica	Valor unitário (R$)	Qtde/Vol	Valor Total(R$)
1					
Valor total estimado da OS					

3 - INSTRUÇÕES/ESPECIFICAÇÕES COMPLEMENTARES

4 - DATAS E PRAZOS PREVISTOS			
Data de Início:		Data do Fim:	
CRONOGRAMA DE EXECUÇÃO			
Item	Execução	Início	Fim
1			

5 - ARTEFATOS	
Fornecidos	A serem gerados e/ou atualizados

6 - ASSINATURA E ENCAMINHAMENTO DA DEMANDA

_____

<Nome >
Fiscal do Contrato
Matr.: <Nº da matrícula>

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – Funpresp-Exe
SCN Quadra 2 Bloco A – Sala 202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 14 DO TERMO DE REFERENCIA

MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

A **FUNPRESP-EXE – FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO FEDERAL DO PODER EXECUTIVO**, sediada em SCN, quadra 02, bloco A, Salas 202/203/204 – Corporate Financial Center | CEP 70712-900 | Brasília-DF, inscrita no CNPJ n° 17.312.597/0001-02 daqui por diante denominada simplesmente CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, representada neste ato por seu(s) representante(s) legal(is) que ao final também assina(m) e se identifica(m), doravante denominada simplesmente **CONTRATADA**, têm justo e acordado o seguinte:

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de definir regras para uso e proteção das informações confidenciais e sigilosas do CONTRATANTE;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições abaixo discriminadas.

CLÁUSULA PRIMEIRA - DO OBJETO - Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações confidenciais e sigilosas, disponibilizadas pela CONTRATANTE - por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes.

CLÁUSULA SEGUNDA - DOS CONCEITOS E DEFINIÇÕES - Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informação Confidencial: informação transmitida pelo CONTRATANTE e recebida pela CONTRATADA, por seus diretores, sócios, administradores, empregados, prepostos ou agentes, sob o poder e propriedade do CONTRATANTE, a qual a CONTRATADA deverá manter em absoluto sigilo, não podendo divulgá-la ou transferi-la a terceiros, sob qualquer forma, bem como não fazer qualquer uso desta para fins diversos dos previstos no Contrato Principal. O acesso a essa informação é baseado na confiança e no estrito cumprimento dos preceitos éticos e legais aplicáveis às atividades do CONTRATANTE, estando ainda, muitas vezes, regulado por compromissos formalmente assumidos com clientes e terceiros, envolvendo riscos financeiros e de imagem incalculáveis.

IV. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.

CLÁUSULA TERCEIRA - DAS INFORMAÇÕES CONFIDENCIAIS - O termo "Informação Confidencial" abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais, dados pessoais e dados pessoais sensíveis de clientes, colaboradores, parceiros e fornecedores, relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro: As INFORMAÇÕES serão identificadas à CONTRATADA por meio da expressão "confidencial" e/ou "reservada".

Parágrafo Segundo: A CONTRATADA se compromete a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Terceiro: A CONTRATADA deverá cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente ou indiretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL. As INFORMAÇÕES devem ser reveladas apenas aos que tiverem necessidade de ter conhecimento sobre elas.

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – Funpresp-Exe
SCN Quadra 2 Bloco A – Sala 202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

Parágrafo Quarto: As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Parágrafo Quinto: A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, diretores, administradores, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto: A CONTRATADA se obriga a não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao CONTRATO PRINCIPAL, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas.

Parágrafo Sétimo: A CONTRATADA se responsabilizará por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros.

Parágrafo Oitavo: A CONTRATADA deverá comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente.

Parágrafo Nono: A CONTRATADA deverá manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – Funpresp-Exe
SCN Quadra 2 Bloco A – Sala 202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

confidenciais, inclusive dados pessoais, devendo comunicar ao CONTRATANTE, imediatamente, até o limite de 48 horas, a ocorrência de incidentes desta natureza, bem como adotar as providências cabíveis, visando à mitigação dos danos, o que não excluirá sua responsabilidade.

Parágrafo Décimo: Fica expressamente proibido que a CONTRATADA se pronuncie em nome do CONTRATANTE perante órgão da Administração Pública Direta e Indireta, perante a imprensa ou qualquer pessoa física ou jurídica, sem a aquiescência prévia, escrita e expressa da administração do CONTRATANTE.

CLÁUSULA QUINTA - DA VIGÊNCIA - O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação das INFORMAÇÕES a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL ou até que estas venham a se tornar de domínio público.

Parágrafo Único: As disposições deste instrumento devem, contudo, ser aplicadas retroativamente a quaisquer INFORMAÇÕES que possam ter sido divulgadas durante a vigência do CONTRATO PRINCIPAL celebrado, antes mesmo da assinatura deste TERMO.

CLÁUSULA SEXTA - DAS PENALIDADES - A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, por ação ou omissão, devidamente comprovada, pela CONTRATADA, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, diretores, administradores, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, possibilitará a imediata aplicação de penalidades, conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. A CONTRATADA, como também o agente causador ou facilitador, estará sujeita à recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

CLÁUSULA SÉTIMA - DA INCOMUNICABILIDADE - Na hipótese de qualquer cláusula ou disposição deste Termo ser declarada nula ou inexequível, tal nulidade ou inexequibilidade não afetará quaisquer outras cláusulas ou disposições aqui contidas, as quais permanecerão em pleno vigor e efeito, desde que o seu objeto não tenha sido alterado ou prejudicado.

CLÁUSULA OITAVA - DA PROPRIEDADE INTELECTUAL - As disposições do presente

Termo não implicam em qualquer licença à CONTRATADA de direitos de utilização e/ou exploração de marcas ou outros bens de propriedade da CONTRATANTE.

CLÁUSULA NONA - DISPOSIÇÕES GERAIS - Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro: Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo: O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo das INFORMAÇÕES.

Parágrafo Terceiro: Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pela CONTRATADA, relativos aos procedimentos e aos controles utilizados na prestação dos serviços objeto do contrato e monitorar as atividades da CONTRATADA, relacionadas ao objeto do contrato;

II. A CONTRATADA deve disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância do CONTRATANTE em exigir o estrito cumprimento das condições estabelecidas neste instrumento configura mera liberalidade, não constituindo novação ou renúncia, nem afetando os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – Funpresp-Exe
SCN Quadra 2 Bloco A – Sala 202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a CONTRATADA, nem como obrigação de celebrarem qualquer outro acordo entre si.

CLÁUSULA DÉCIMA - DO FORO - O CONTRATANTE elege o foro da cidade de Brasília-DF, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

CLÁUSULA DÉCIMA PRIMEIRA - Os dados pessoais e dados pessoais sensíveis, definidos na forma da Lei Geral de Proteção de Dados – nº 13.709/18, aos quais a CONTRATADA terá acesso estão salvaguardados pela referida Lei e devem, especialmente, ser tratados de forma confidencial, observando-se os preceitos da legislação e as obrigações assumidas contratualmente, inclusive no que tange a sua forma de proteção, utilizando dos meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

C O N T R A T A N T E

_____

FUNPRESP-EXE - FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR DO SERVIDOR PÚBLICO FEDERAL DO PODER EXECUTIVO

C O N T R A T A D A

_____

EMPRESA

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – Funpresp-Exe
SCN Quadra 2 Bloco A – Sala 202/203/204 – Ed. Corporate Financial Center – Brasília – DF / 70712-900 - (061) 2020-9700
www.funpresp.com.br

ANEXO 15 DO TERMO DE REFERENCIA

MODELO DE TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

1 – IDENTIFICAÇÃO			
Contrato nº			
Objeto do Contrato			
Contratada		**CNPJ**	
Preposto			
Gestor do Contrato		**Matrícula**	

2 - CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**

ANEXO 16 DO TERMO DE REFERENCIA

À

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo

Edifício Corporate Financial Center - SCN - Quadra 02 – Bloco A – 2º Andar – Salas 201 a 204 – Brasília – DF – CEP: 70712-900

CNPJ nº 17.312.597/0001-02

Validade da Proposta: 90 (noventa) dias.

Assunto: PLANILHA DE COMPOSIÇÃO DE CUSTOS.

1. Na Proposta Comercial, em papel timbrado, deverão ser informadas as marcas, modelos e quantidades de todos os produtos, peças ou softwares necessários à correta prestação dos serviços, assim como a descrição de como será feito o atendimento aos requisitos deste Termo de Referência, nos seguintes termos:

   a) as especificações dos materiais/softwares ofertados;
   b) características técnicas;
   c) acessórios normais;
   d) acessórios opcionais;
   e) marca;
   f) modelo e/ou referência;
   g) prazo de entrega;
   h) prazo de garantia (mínimo de 60 meses); e
   i) documentos comprobatórios da origem dos materiais ou softwares, da matéria prima e/ou dos componentes

2. Nos preços apresentados deverão estar incluídas todos os custos diretos e indiretos, e despesas com materiais, mão-de-obra, links, deslocamentos, manutenção corretiva, hospedagens, ferramentas, equipamentos, seguros, taxas, tributos, incidências fiscais e contribuições de qualquer natureza ou espécie, encargos sociais, salários, deslocamentos, hospedagens, e quaisquer outros encargos necessários à perfeita execução do objeto da licitação.

3. Data e assinatura do representante da empresa.

4. Tabela de valores:

GRUPO	ITEM	DESCRIÇÃO	QTD	UN	VALOR UNITÁRIO	VALOR 36 MESES
1	1	**SERVIÇO DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES**	36	MESES		
	2	**SERVIÇO DE GESTÃO DE VULNERABILIDADES**	36	MESES		
	3	**SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS**	36	MESES		
	4	**SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA**	36	MESES		
	5	**SERVIÇO DE PROTEÇÃO DE TRÁFEGO DE BORDA**	36	MESES		
	6	**SERVIÇO DE INTELIGÊNCIA APLICADA À SEGURANÇA**	36	MESES		
	7	**SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO**	36	MESES		
2	1	**SERVIÇOS TÉCNICOS ESPECIALIZADOS**	1440	HORAS		
3	1	**SERVIÇO DE TESTES DE INVASÃO**	36	MESES		
TOTAL						

Preço Unitário por Extenso:

Preço Total por Extenso:

ANEXO 17 DO TERMO DE REFERENCIA

Assunto: PLANILHA DE VERIFICAÇÃO DE ADEQUAÇÃO

Grupo 01	
Item de verificação	Solução proposta
Endereço físico do Datacenter	
Ferramenta de descoberta de Vulnerabilidades	
Ferramenta de Gestão de Vulnerabilidades	
Solução para blindagem de aplicações WEB (WAF)	
Ferramenta SIEM	
Solução para gerenciamento de incidentes de segurança da informação	
Solução ITSM	
Ferramenta de proteção de endpoint (EDR)	
Ferramenta para campanhas de phishing	

Grupo 03	
Item de verificação	Solução proposta
Ferramenta a ser utilizada para a execução dos testes de invasão	

Contrato n. 5 para assinatura InterOp.pdf

Documento número #5b18a7a4-f38e-49b0-83a2-82cfa2313cd7

Hash do documento original (SHA256): 2e913df2cc3554ceb965593909f24fd2d951b8b17afb66d87a8fff1566a0b757

Assinaturas

Fabiane de Sousa Dumont
CPF: 005.987.071-07
Assinou como testemunha em 05 abr 2024 às 15:02:41

Ibsen Naezio Alves Aguiar
CPF: 043.308.441-33
Assinou como testemunha em 08 abr 2024 às 12:11:35

Cícero Rafael Barros Dias
CPF: 629.731.263-04
Assinou como contratante em 08 abr 2024 às 08:22:30

Cleiton dos Santos Araújo
CPF: 851.631.201-15
Assinou como contratante em 05 abr 2024 às 19:42:21

Sócrates Slongo
CPF: 512.537.040-15
Assinou como contratada em 08 abr 2024 às 08:43:42

Log

05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 criou este documento número 5b18a7a4-f38e-49b0-83a2-82cfa2313cd7. Data limite para assinatura do documento: 05 de maio de 2024 (14:48). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 adicionou à Lista de Assinatura: fabiane.dumont@funpresp.com.br para assinar como testemunha, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Fabiane de Sousa Dumont e CPF 005.987.071-07.

05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 adicionou à Lista de Assinatura: ibsen.aguiar@funpresp.com.br para assinar como testemunha, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Ibsen Naezio Alves Aguiar e CPF 043.308.441-33.
05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 adicionou à Lista de Assinatura: cicero.dias@funpresp.com.br para assinar como contratante, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Cícero Rafael Barros Dias e CPF 629.731.263-04.
05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 adicionou à Lista de Assinatura: cleiton.araujo@funpresp.com.br para assinar como contratante, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Cleiton dos Santos Araújo e CPF 851.631.201-15.
05 abr 2024, 14:53:40	Operador com email fabiane.dumont@funpresp.com.br na Conta 5a7ad025-01a9-4c15-ba9e-30a8be81b5c5 adicionou à Lista de Assinatura: socrates@interop.com.br para assinar como contratada, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Sócrates Slongo e CPF 512.537.040-15.
05 abr 2024, 15:02:41	Fabiane de Sousa Dumont assinou como testemunha. Pontos de autenticação: Token via E-mail fabiane.dumont@funpresp.com.br. CPF informado: 005.987.071-07. IP: 189.85.93.162. Componente de assinatura versão 1.809.0 disponibilizado em https://app.clicksign.com.
05 abr 2024, 19:42:21	Cleiton dos Santos Araújo assinou como contratante. Pontos de autenticação: Token via E-mail cleiton.araujo@funpresp.com.br. CPF informado: 851.631.201-15. IP: 189.85.93.162. Localização compartilhada pelo dispositivo eletrônico: latitude -15.7915298 e longitude -47.8921573. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.809.0 disponibilizado em https://app.clicksign.com.
08 abr 2024, 08:22:30	Cícero Rafael Barros Dias assinou como contratante. Pontos de autenticação: Token via E-mail cicero.dias@funpresp.com.br. CPF informado: 629.731.263-04. IP: 189.85.93.162. Componente de assinatura versão 1.809.0 disponibilizado em https://app.clicksign.com.
08 abr 2024, 08:43:42	Sócrates Slongo assinou como contratada. Pontos de autenticação: Token via E-mail socrates@interop.com.br. CPF informado: 512.537.040-15. IP: 200.175.93.135. Localização compartilhada pelo dispositivo eletrônico: latitude -30.029434 e longitude -51.234196. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.809.0 disponibilizado em https://app.clicksign.com.
08 abr 2024, 12:11:35	Ibsen Naezio Alves Aguiar assinou como testemunha. Pontos de autenticação: Token via E-mail ibsen.aguiar@funpresp.com.br. CPF informado: 043.308.441-33. IP: 189.85.93.162. Localização compartilhada pelo dispositivo eletrônico: latitude -15.791529 e longitude -47.8940113. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.811.0 disponibilizado em https://app.clicksign.com.
08 abr 2024, 12:11:36	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 5b18a7a4-f38e-49b0-83a2-82cfa2313cd7.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 5b18a7a4-f38e-49b0-83a2-82cfa2313cd7, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.