



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

### ANEXO II – ESPECIFICAÇÕES TÉCNICAS PROCESSO ADMINISTRATIVO Nº 0140/2023

As especificações técnicas mínimas da Solução a ser contratada seguem descritas abaixo:

#### 1. GERAL, AMOSTRA E COMPROVAÇÃO DE ATENDIMENTO

**1.1.** As soluções ofertadas deverão ser plenamente integráveis, não podendo apresentar nenhum tipo de incompatibilidade;

**1.2.** A CONTRATADA deverá possuir processos implementados que garantem a segurança das informações da CONTRATANTE, em conformidade com a Norma ABNT NBR ISO/IEC 27001 e ISSO 27701.

**1.3.** Deverão ser utilizados os seguintes padrões de mercado para execução dos serviços:

**1.3.1.** OWASP Testing Guide: a Open Web Application Security Project (OWASP) fornece uma ampla gama de recursos, incluindo o OWASP Testing Guide, que é um guia prático e abrangente para testes de segurança de aplicativos da web.

**1.3.2.** PTES (Penetration Testing Execution Standard): O PTES é uma iniciativa destinada a criar um padrão para a execução e relatório de testes de penetração.

**1.3.3.** NIST SP 800-115: Este documento do National Institute of Standards and Technology (NIST) dos EUA fornece orientações sobre a realização de testes de penetração em sistemas de informação.

**1.4.** Deverá existir comprovação de que a licitante fornece/forneceu solução de natureza semelhante ou compatível com o objeto desta contratação.

**1.5.** A comprovação será feita por meio de apresentação de atestados ou cópias de contratos, conforme abaixo:

**1.5.1.** Atestados:

**1.5.1.1.** Fornecidos por empresa de direito público ou privado;

**1.5.1.2.** O(s) atestado(s) de capacidade técnica deverá(ão) conter as informações:

- a)** Nome da empresa atestante, endereço, CNPJ, contatos (nome, cargo, telefone);
- b)** Descrição do objeto, de forma a possibilitar ao Coren-SP o entendimento dos trabalhos realizados, bem como a aferição da compatibilidade com o objeto da presente contratação.

**1.5.2.** Cópias de Contratos:

**1.5.2.1.** Cópias de contratos, comprovando que a licitante fornece/forneceu solução de natureza semelhante e/ou compatível com o objeto desta contratação, no âmbito de sua atividade econômica principal e/ou secundária especificada no seu contrato social.

**1.5.2.2.** A licitante deverá disponibilizar, quando solicitado, todas as informações necessárias à comprovação da legitimidade dos atestados de capacidade técnica apresentados.

**1.6.** Deverá a empresa CONTRATADA apresentar ao menos um certificado abaixo de profissional que



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

compõe sua equipe de pentest e análise de vulnerabilidade. Além disso, os relatórios devem ser assinados também por profissional com uma das certificações mencionadas:

**1.6.1.** OSCP (Offensive Security Certified Professional): Oferecido pela Offensive Security, o OSCP é uma das certificações mais reconhecidas para profissionais de Red Team. Ela envolve um exame prático desafiador, em que os candidatos devem penetrar em uma série de máquinas virtuais para demonstrar suas habilidades técnicas de penetração.

**1.6.2.** OSCE (Offensive Security Certified Expert): Também da Offensive Security, é uma certificação avançada focada em técnicas de exploração e desenvolvimento de exploits. É voltada para profissionais que desejam aprimorar suas habilidades de análise de vulnerabilidades e criação de exploits.

**1.6.3.** CREST CRT (Certified Red Team Member): Oferecido pelo CREST (Council of Registered Ethical Security Testers), esta certificação valida habilidades técnicas de testes de invasão e Red Team, além de conhecimentos em metodologia e ética de testes.

**1.6.4.** CEH (Certified Ethical Hacker): Oferecido pela EC-Council, é uma certificação amplamente conhecida que abrange os fundamentos da segurança de redes e as práticas de hacking ético.

**1.6.5.** CompTIA PenTest+: Esta certificação abrange habilidades em testes de penetração em vários ambientes e sistemas. É uma boa certificação de nível intermediário para profissionais que desejam entrar na área.

**1.6.6.** GIAC Penetration Tester (GPEN): Oferecido pela Global Information Assurance Certification (GIAC), é uma certificação focada em habilidades de pentest e testes de segurança de aplicativos.

**1.6.7.** LPT (Licensed Penetration Tester): Oferecido pela EC-Council, é uma certificação avançada que valida as habilidades práticas de um pentester em um ambiente controlado.

**1.7. Quantidade de Horas de Pentest e Engenharia Social:** Para os serviços de pentest e engenharia social, serão contratadas até 1500 (mil e quinhentas) horas para uso sob demanda, que poderão ser utilizadas em qualquer um dos serviços, sob demanda da CONTRATANTE.

**1.8. Quantidade de Dispositivos para a Análise de Vulnerabilidades:** O scan e mapeamento de rede IP que será realizado para a prestação de serviço internamente tem como estimativa os seguintes dispositivos e quantidades para o primeiro scan (scan total) e scans subsequentes (scans parciais):

**1.8.1.** Para o serviço de análise de vulnerabilidades, será contratada análise de até 1600 dispositivos para o scan total (equivalente aos 1460 dispositivos atualmente no ambiente mais uma projeção aproximada de crescimento para os próximos meses).

**1.8.2.** Na tabela abaixo também são listadas as porcentagens para escopo dos scans subsequentes (scans parciais), onde não será necessária a análise total de todos os hosts do ambiente do Coren-SP;

**1.8.3.** Para os scans subsequentes (scans parciais), entende-se que não há necessidade de escaneamento total, sendo realizados scans por amostragem, conforme porcentagens abaixo, totalizando 233 dispositivos por scan parcial e, conforme a projeção de aumento do scan total, representando até 300 dispositivos a serem analisados em cada scan parcial, sendo assim, um total de 900 dispositivos:

Item	Quantidade total para o 1º scan (scan total)	Percentual a partir do 2º scan (scan	Quantidade a partir do 2º scan, por scan (scan parcial)
------	--	--------------------------------------	---



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

		parcial)	
Tablets	250	5%	12
Servidores virtuais	55	100%	55
Servidores físicos	15	100%	15
Desktops / Notebooks	650	5%	32
Impressoras	67	10%	6
Scanners	7	5%	0
Switches na sede	16	100%	16
Switches nas subseções	31	100%	31
Access Points WiFi	50	20%	10
Switch Core	2	100%	2
Catracas e travas físicas	45	10%	4
Câmeras	230	10%	23
Relógio de Ponto	17	15%	2
Controladora WiFi	1	100%	1
Firewalls na sede	2	100%	2
Firewalls nas subseções	18	100%	18
Storage	1	100%	1
Biblioteca de fita	1	100%	1
Nobreaks	2	100%	2
Subtotal	1460	-	233
<b>TOTAL com Projeção de crescimento</b>	<b>1600</b>	<b>-</b>	<b>300</b>

**1.9.** O presente documento especificará as soluções a serem contratadas;

**1.10.** Considera-se ativos escopo desses serviços, qualquer item de configuração de TI, podendo ser endpoint, hosts, dispositivos de rede e comunicação, aplicação web interna, interface de aplicação ou sistema desenvolvido internamente, entre outros.

**1.10.1.** Número aproximado de aplicações e sistemas web internos no Coren-SP: 70 (setenta);

**1.11.** As propostas no pregão deverão incluir demonstração de cumprimento de cada um dos itens da especificação. Itens que não seja possível a demonstração, devem possuir declaração expressa da licitante, informando cumprir o item em sua totalidade.

**1.12.** A contratada e seus colaboradores envolvidos no projeto devem firmar um Termo de Confidencialidade junto ao Coren-SP, o qual será disponibilizado após a formalização do contrato. O compartilhamento de informações obtidas durante as análises e testes realizados no ambiente do Coren-SP não é permitido.

**1.13.** O pagamento das horas utilizadas será realizado mensalmente, nos meses em que ocorrer sua utilização, após emissão de relatório mensal por parte da CONTRATADA e comprovação das atividades executadas, por meio dos relatórios referidos nos itens anteriores.

## **2. SERVIÇO DE ANÁLISE DE VULNERABILIDADES**

**2.1.** A CONTRATADA deve eliminar os falsos positivos e as vulnerabilidades não aplicáveis ao ambiente



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

da CONTRATANTE para a geração dos relatórios e das recomendações;

**2.2.** A CONTRATADA deverá tomar as providências necessárias para evitar que as análises causem indisponibilidades ou alterações no ambiente do CONTRATANTE;

**2.3.** Quando necessário, o CONTRATANTE poderá solicitar um maior detalhamento de itens específicos dos relatórios.

**2.4.** Os relatórios deverão estar em português.

**2.5.** A CONTRATADA deverá executar o serviço dentro dos níveis de acordo de serviço (SLA) explicitados abaixo, incorrendo em glosas sobre o valor da fatura (VF) conforme a tabela a seguir:

Indicador	Objetivo	Fórmula de Cálculo	Resultado Aceitável	Redutor
Entrega dos relatórios	Entregar os relatórios exigidos no prazo acordado.	Por dia de atraso	Atraso = 0 dias	5% do VF por ocorrência (+5% por semana extra de atraso, limitado a 15%, por relatório)

**2.6.** As seguintes ocorrências também serão objeto de glosa no valor da fatura (VF), limitados até 40%, no caso da CONTRATADA:

Descrição	Referência	Redutor
Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	10% do VF
Suspender, colocar como pendente ou interromper, salvo por motivo justificado, a execução dos serviços.	Por ocorrência	5% do VF
Realizar mudanças de configuração nos ativos de Cybersegurança sem autorização da CONTRATANTE.	Por ocorrência	10% do VF
Fraudar, manipular ou descaracterizar indicadores de níveis de serviço e de desempenho por quaisquer subterfúgios	Por ocorrência	20% do VF
Recusar-se a executar serviço relacionado às atividades deste ITEM solicitado pela CONTRATANTE.	Por ocorrência	10% do VF

**2.7.** O pagamento ocorrerá, após a avaliação do nível de serviço conforme relatórios elencados no item anterior e no termo de referência e computadas às eventuais glosas do mês de referência.

**2.8.** “Análise de Vulnerabilidades” ou “Vulnerability Assessment”: estas atividades basicamente visam o descobrimento e mapeamento de acessos, topologias, sistemas e vulnerabilidades, sem executar nenhuma ação de exploração que possa causar interrupção dos serviços, degradação de acessos ou adulteração de informações, onde serão dados os acessos necessários para que a CONTRATADA realize as varreduras e a emissão de relatórios técnicos.



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

**2.9.** A contratada deve dispor de todos os recursos para a realização das análises e testes, ficando o Coren-SP obrigado apenas a providenciar acesso a infraestrutura para realização dos preparativos e dos testes propriamente ditos.

**2.10.** O Coren-SP solicitará nova análise, nos mesmos moldes e com os mesmos prazos da análise de vulnerabilidades, para minimamente aferir as remediações sugeridas pelos relatórios técnicos anteriores além de eventuais outras descobertas, até 3 meses após a finalização da apresentação de resultados. Sendo esse o prazo para solução das vulnerabilidades críticas apontadas pelo serviço, por parte das equipes internas do Coren-SP.

**2.11.** Neste serviço, a execução concentra-se na avaliação do ambiente interno de tecnologia da informação do Coren-SP, com a flexibilidade de ser executada tanto de forma presencial quanto remota.

**2.12.** A análise de vulnerabilidades, componente central destes serviços, pode ser conduzida de maneira presencial, nas instalações do Coren-SP, ou de forma remota, com o método de conexão a ser acordado entre o Coren-SP e a CONTRATADA, desde que de forma segura e desde que autorizado pela CONTRATANTE.

**2.12.1.** O Coren-SP possui autonomia para exigir que os testes sejam feitos de forma remota, ficando obrigado a prover acesso remoto ao ambiente interno para a CONTRATADA realizar os serviços.

**2.13.** Visando a execução eficaz dos serviços, a CONTRATADA poderá implementar ferramentas especializadas em análise de vulnerabilidades no ambiente do Coren-SP, respeitando as diretrizes de segurança e sigilo.

**2.14.** Para garantir a adequação da proposta, a CONTRATADA deve considerar os parâmetros listados abaixo, destinados a esclarecer possíveis dúvidas relacionadas à elaboração dos serviços:

**2.14.1.** Avaliação dos serviços externos de TI, bem como dos servidores, firewalls e outros componentes integrantes dos sistemas de proteção;

**2.14.2.** Análise de aplicações web, englobando portais, sites e sistemas web;

**2.14.3.** Realização de sondagem e mapeamento de rede;

**2.14.4.** Varredura das portas e dos serviços em execução;

**2.14.5.** Identificação das rotas, dos dispositivos e dos sistemas operacionais.

**2.15.** A metodologia deve abranger tanto abordagens automatizadas quanto manuais, coletando informações que sustentem a identificação e a exploração de vulnerabilidades.

**2.16.** A CONTRATADA deve:

**2.16.1.** Avaliar elementos ativos expostos na rede pública, como firewalls, roteadores, IPS, filtros, proxies e autenticadores;

**2.16.2.** Identificar serviços privilegiados desprotegidos e potenciais backdoors;

**2.16.3.** Instalar coletores de pacotes (packet sniffers) e outras ferramentas de monitoramento, quando aplicável;

**2.16.4.** Detectar vulnerabilidades em relação à personificação de máquinas confiáveis (trusted hosts) e anomalias de roteamento;

**2.16.5.** Identificar possíveis vulnerabilidades de adulteração do DNS (DNS spoofing);



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 2.16.6.** Avaliar falhas em Web Servers, FTP Servers, Mail Servers e DNS Servers;
- 2.16.7.** Identificar vulnerabilidades associadas a aplicações web expostas ao público;
- 2.16.8.** Analisar se falhas de segurança nas aplicações possibilitam interação com recursos do sistema operacional e do banco de dados;
- 2.16.9.** Verificar o comportamento das aplicações em relação aos sistemas operacionais, identificando falhas que possam ser exploradas por usuários com acesso aos sistemas, porém não autenticados pelas aplicações.

**2.17.** Salienta-se a necessidade de que as atividades executadas transcendam a mera utilização de ferramentas, abarcando procedimentos e técnicas não abrangidos por ferramentas conhecidas.

**2.18.** A CONTRATADA tem a responsabilidade de não alterar a integridade das informações, assegurando que servidores e sistemas permaneçam inalterados a fim de não comprometer os serviços prestados pelo Coren-SP.

**2.19.** Importa, também, identificar todas as aplicações presentes em cada host a ser analisado. Uma vez descobertas e identificadas, todas as etapas de análise e exploração devem ser aplicadas a cada uma dessas aplicações.

**2.20.** Ao concluir o trabalho, a CONTRATADA deverá apresentar todos os artefatos, documentação, relatórios, manuais e demais materiais que validem a execução das atividades nesta fase. Em sequência, será fornecido um Termo de Aceite ao Coren-SP, que verificará a conformidade dos serviços com as necessidades preestabelecidas.

**2.21.** O Coren-SP, por sua vez, poderá apontar correções caso considere que os serviços prestados e os artefatos apresentados não atendam ao escopo desta fase. Em situações em que correções sejam necessárias, o Coren-SP indicará quais produtos, ativos ou serviços precisam ser ajustados.

**2.22.** Se as correções efetuadas pela CONTRATADA ainda apresentarem falhas, o Coren-SP não poderá assinar o Termo de Aceite até que as devidas correções sejam implementadas.

**2.23.** Os serviços de análise de vulnerabilidades, conduzidos no ambiente externo de tecnologia do Coren-SP, devem ser realizados em uma única ocasião, com o propósito de identificar, de maneira pro-ativa, possíveis falhas e vulnerabilidades de segurança em ativos de rede, bancos de dados, aplicações web, servidores e serviços de TIC do Coren-SP, visando mitigar a probabilidade de ataques cibernéticos direcionados à instituição por meio da exploração das vulnerabilidades encontradas.

**2.24.** Esta fase tem como especificação o serviço de verificação e identificação de falhas e vulnerabilidades externas de segurança da informação já catalogadas e reconhecidas, baseadas na lista pública de falhas de segurança da informação denominada CVE (Common Vulnerabilities and Exposures), a qual notifica e orienta sobre os procedimentos necessários para a mitigação das vulnerabilidades a fim de sanar possíveis brechas de segurança.

**2.25.** Para a análise e varredura dos ativos e serviços de tecnologia, a CONTRATADA deve atender aos seguintes requisitos:

- 2.25.1.** Identificar e analisar os sistemas operacionais;
- 2.25.2.** Realizar varredura por endereço IP, sistema operacional, nome DNS, nome NetBIOS ou nome de domínio.

**2.26.** A CONTRATADA deve gerar um relatório no formato PDF para cada ativo ou serviço avaliado, contendo, no mínimo, as seguintes informações para cada vulnerabilidade identificada:



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 2.26.1.** Descrição;
- 2.26.2.** Nível de severidade;
- 2.26.3.** Exploits disponíveis;
- 2.26.4.** Referências e links para fontes de informações sobre a vulnerabilidade;
- 2.26.5.** Medidas de remediação;
- 2.26.6.** Detalhes e evidências da vulnerabilidade.

**2.27.** Caso correções sejam necessárias nas informações contidas no relatório, o Coren-SP deverá comunicar a CONTRATADA, fornecendo um registro escrito das inconsistências observadas. A CONTRATADA deverá corrigir essas inconsistências e encaminhar o relatório revisado em até 3 (três) dias úteis após a notificação por escrito feita pelo Coren-SP.

**2.28.** Tanto ferramentas de análise de vulnerabilidades quanto técnicas manuais de análise devem ser empregadas. A CONTRATADA deve submeter as ferramentas a serem utilizadas a uma revisão prévia e obter a aprovação do Coren-SP antes de sua efetiva aplicação. O mesmo procedimento aplica-se à metodologia para análise manual de vulnerabilidades.

**2.29.** Os requisitos abaixo devem ser atendidos e apresentados no relatório:

- 2.29.1.** Coleta Passiva, englobando no mínimo as seguintes técnicas:
  - 2.29.1.1.** Whois e nslookup (consultas DNS);
  - 2.29.1.2.** Sites de busca;
  - 2.29.1.3.** Listas de discussão;
  - 2.29.1.4.** Blogs colaborativos;
  - 2.29.1.5.** Informações disponíveis publicamente;
  - 2.29.1.6.** Passive eavesdropping (captura passiva de pacotes);
  - 2.29.1.7.** Captura de banners.
- 2.29.2.** Coleta Ativa, englobando no mínimo as seguintes técnicas:
  - 2.29.2.1.** Mapeamento de rede (port scanning);
  - 2.29.2.2.** Varredura de vulnerabilidades.

**2.30.** A varredura de vulnerabilidades deve abranger, entre outros:

- 2.30.1.** Identificação de hosts ativos na rede;
- 2.30.2.** Identificação de portas e serviços em execução;
- 2.30.3.** Detecção de serviços ativos e vulneráveis nos hosts;
- 2.30.4.** Análise de sistemas operacionais;
- 2.30.5.** Identificação de vulnerabilidades associadas a sistemas operacionais e aplicações descobertas;
- 2.30.6.** Avaliação das configurações de segurança inadequadas nos hosts;
- 2.30.7.** Identificação de rotas e estimativa do impacto em caso de modificações/desconfigurações;



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 2.30.8.** Identificação de vetores de ataque e cenários de exploração;
  - 2.30.9.** Detecção de vulnerabilidades reconhecidas (CVE);
  - 2.30.10.** Classificação de vulnerabilidades por risco (alto, médio, baixo);
  - 2.30.11.** Informações relevantes para a fase de ataques.
- 2.31.** No âmbito dos serviços e aplicações web, a análise deve abranger:
- 2.31.1.** Uso inadequado de sistemas de arquivos e arquivos temporários;
  - 2.31.2.** Manipulação de informações devido a configurações de tratamento de erros padrão;
  - 2.31.3.** Tratamento impróprio de entradas;
  - 2.31.4.** Questões relacionadas a configurações inadequadas dos serviços;
  - 2.31.5.** Gerenciamento inseguro de sessões web.
- 2.32.** A Análise de vulnerabilidades deverá ser realizada abrangendo no mínimo o seguinte escopo:
- 2.32.1.** Encontrar vulnerabilidades associadas a aplicações existentes na rede interna;
  - 2.32.2.** Analisar a segurança dos sistemas indicados em conformidade com as melhores práticas utilizadas pelo mercado, tais como OWASP – The Open Web Application Security Project ([www.owasp.org](http://www.owasp.org));
  - 2.32.3.** A solução usada deve possuir capacidade de descoberta e geração de inventário de servidores e demais dispositivos e serviço web, através do rastreamento (crawling) de servidores Web e seus conteúdos, a fim de identificar e analisar seu conteúdo, resultando em uma lista categorizada de servidores web e os objetos que residem neles, como também nos ativos de infraestrutura de rede;
    - 2.32.3.1.** São incluídas até 30 VLANs no ambiente e que devem participar das análises.
  - 2.32.4.** Mapeamento do parque de ativos de TI com possibilidade de identificação de equipamentos não autorizados (“shadow IT”);
- 2.33.** Para fins de dimensionamento da proposta, a CONTRATADA deverá utilizar os parâmetros elencados abaixo, além dos itens anteriores, a fim de sanar possíveis dúvidas para o dimensionamento dos serviços a serem executados.
- 2.34.** O quantitativo e tipos de dispositivos estão listados em tabela geral em item anterior deste Termo de Referência;
- 2.35.** O relatório da Análise de Vulnerabilidades deve informar, no mínimo, os seguintes detalhes:
- 2.35.1.** Sumário executivo. Entende-se por sumário executivo como parte inicial do relatório que se dedica a resumir as descobertas, impactos e recomendações do trabalho numa visão geral concisa e de alto nível e em linguagem não-técnica.
  - 2.35.2.** Descrição de ferramentas e metodologias utilizadas;
  - 2.35.3.** Apresentação dos resultados baseados em ordem de criticidade (do mais crítico para o menos crítico). A criticidade a ser empregada deverá ser o padrão Common Vulnerability Scoring System (CVSS).
  - 2.35.4.** IP do recurso computacional (quando possível);





## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 2.35.5.** Nome do recurso computacional (quando possível);
  - 2.35.6.** Descrição do ativo (se possível);
  - 2.35.7.** Nível de criticidade (alta, média ou baixa);
  - 2.35.8.** Origem da ação realizada internamente/externamente(I/E);
  - 2.35.9.** Data da execução da atividade;
  - 2.35.10.** Descrição das vulnerabilidades (CVE, data de registro da vulnerabilidade etc..)
  - 2.35.11.** Evidências;
  - 2.35.12.** Análise de impacto – categorização e ponderação de ameaças;
  - 2.35.13.** Procedimentos de correção ou contramedidas recomendadas pela equipe especializada da CONTRATADA;
  - 2.35.14.** Mapeamento de redes, equipamentos e sistemas;
  - 2.35.15.** Não serão aceitos relatórios gerados exclusivamente por ferramentas automatizadas e softwares especializados;
- 2.36.** Além do relatório técnico apresentado acima, a CONTRATADA deve apresentar planilha contendo os dados do relatório de forma a facilitar o trabalho de seleção e ordenação dos resultados para o Coren-SP posteriormente.;
- 2.37.** Os relatórios técnicos e planilhas deverão ser entregues obrigatoriamente em meio eletrônico e de forma segura, que garanta a confidencialidade e não vazamento das informações contidas no relatório e seus anexos;

### 3. SERVIÇO DE PENTEST E ENGENHARIA SOCIAL

#### 3.1. PENTEST

- 3.1.1.** A CONTRATADA deverá realizar serviços de testes de intrusão (pentest), sob demanda, a determinados ativos do ambiente de TI da CONTRATANTE, com o objetivo de identificar e explorar vulnerabilidades de forma controlada, simulando ataques reais realizados por profissionais certificados e capacitados, devendo incluir a elaboração e apresentação de relatórios detalhados contendo os métodos, técnicas e ferramentas utilizados bem como avaliação, diagnóstico e recomendações de correção das vulnerabilidades encontradas durante a realização dos testes.
- 3.1.2.** Para os serviços de Pentest, serão contratadas até 1.500 (mil e quinhentas) horas para uso sob demanda durante a vigência do contrato.
- 3.1.2.1.** Serão testados 16 (dezesesseis) endereços externos de internet (páginas web e VPN) e 4 SSIDs de wi-fi;
  - 3.1.2.2.** Os testes realizados serão do tipo graybox ou outro acordado entre as partes na reunião de planejamento;
- 3.1.3.** O quantitativo de horas acima especificado trata-se de valor de referência para fins de contratação. O pagamento será realizado apenas para as horas efetivamente utilizadas.
- 3.1.4.** O escopo do serviço e a quantidade de horas estimada para a execução dos testes deve ser previamente informada e alinhada junto aos gestores da CONTRATANTE. Tal serviço deve ser formalizado por meio da Ordem de Serviço pela CONTRATANTE através de e-mail ou em formato a ser acordado junto a CONTRATADA.



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

**3.1.5.** O horário para a execução dos testes de intrusão na infraestrutura de TI da CONTRATANTE poderá ser fora do horário comercial, inclusive em dias não úteis, a critério da CONTRATANTE.

**3.1.6.** Os pentests serão executados em aplicações de internet (externas) e em redes Wi-Fi. Os tipos de Pentest a serem realizados podem ser destinados a aplicações Web ou em Nuvem, APIs, Banco de Dados ou outros alvos a serem definidos pela CONTRATANTE.

**3.1.7.** Os testes devem ser realizados somente com a autorização formal da CONTRATANTE nas modalidades existentes de mercado, podendo ser com informações completas, parciais ou sem detalhamento, anunciado ou não anunciado às equipes internas, bem como interno, externo ou em um ponto específico;

**3.1.8.** Os testes (pentest), dependendo do escopo escolhido pela CONTRATANTE, poderão ser aplicados nos seguintes formatos:

**3.1.8.1.** Metodologia de ataques cibernéticos envolvendo tecnologias de rede e protocolos utilizando varreduras automatizadas de descoberta e específicas de vulnerabilidades técnicas, incluindo ataque de acesso remoto (wireless e vpn), infraestrutura (firewall, IPS, WAF, entre outros), bancos de dados e sistemas operacionais (Windows, Linux, iOS e Android);

**3.1.8.2.** Metodologia de ataques cibernéticos envolvendo varreduras de aplicação, incluindo injeção de código em páginas, formulários web e as listadas no OWASP top 10 Application Security Risks vigente.

**3.1.8.3.** Metodologia de ataques cibernéticos envolvendo varreduras de APIs, incluindo as listadas no OWASP API Security vigente e linguagens de programação WEB (.Net, ASP, Java, JavaScript, PHP, Python).

**3.1.9.** Deve ser realizada avaliação técnica da configuração de segurança (hardening) dos ativos, indicando sua aderência aos padrões internacionais estabelecidos pelo NIST/CIS/FIRST, observando os processos de:

**3.1.9.1.** Autenticação, sugerindo os devidos controles de segurança para o repouso, processamento e transferência de credenciais (usuário e senha) para o ambiente alvo da análise;

**3.1.9.2.** Autorização, considerando as permissões e grupos de privilégio necessários àquele ativo;

**3.1.9.3.** Auditoria, recomendando os IDs dos eventos importantes para serem registrados e armazenados para investigações de ataques;

**3.1.9.4.** Serviços, elencar os serviços e protocolos desnecessários ao funcionamento do ativo para a sua determinada função no ambiente;

**3.1.9.5.** Outros pontos pertinentes a prática de hardening.

**3.1.10.** As técnicas adotadas deverão ter ênfase na compreensão das características dos recursos previamente indicados pela CONTRATANTE considerando a integridade, confidencialidade e disponibilidade dos recursos e dados.

**3.1.11.** A exploração das vulnerabilidades deve ser realizada após autorização formal da CONTRATANTE para ação coordenada junto aos profissionais indicados pela CONTRATANTE, em datas e horários acordados;



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

**3.1.12.** Os resultados das explorações das vulnerabilidades deverão ser documentados com a coleta de evidências suficientes para comprovar o êxito na exploração do ambiente;

**3.1.13.** As vulnerabilidades encontradas devem ser apresentadas com a classificação do nível de risco utilizando a metodologia CVSS – Common Vulnerability Scoring System do FIRST, contendo:

**3.1.13.1.** A descrição e análise das métricas bases:

- a) Vetor de ataque
- b) Complexidade do ataque
- c) Privilégios requeridos
- d) Iteração com um usuário
- e) Impacto na confidencialidade, integridade e disponibilidade do ativo

**3.1.13.2.** A descrição e análise das métricas temporais:

- a) Maturidade do código de exploração (exploit)
- b) Nível de remediação
- c) Confidencialidade

**3.1.13.3.** A descrição e análise da métrica específica do ambiente da CONTRATANTE:

- a) Mitigações existentes na CONTRATANTE
- b) Impacto nos serviços críticos da CONTRATANTE (confidencialidade, integridade e disponibilidade).

**3.1.14.** As recomendações deverão ser especificadas para a solução de cada uma das falhas identificadas.

**3.1.15.** As recomendações devem ser priorizadas considerando a evolução de maturidade do ambiente de infraestrutura da CONTRATANTE e no caso de encontrar vulnerabilidades críticas com CVSS acima de 9, as mesmas deverão ser reportadas imediatamente a CONTRATANTE;

**3.1.16.** A gerência dos testes deve ser realizada pela CONTRATADA de acordo com práticas de mercado para gestão de projetos;

**3.1.17.** O serviço deverá ser realizado preferencialmente de forma remota. Ações locais devem somente ser realizadas quando fundamental para execução de testes específicos que requerem acesso local;

**3.1.18.** O prazo para mitigar as vulnerabilidades e início da realização do reteste sem custo à CONTRATANTE deve ser de 3 meses.

**3.1.19.** A distribuição das horas conforme mencionado anteriormente dependerá dos cenários acordados entre a empresa contratada e a contratante.

**3.1.20.** Qualquer atividade que apresente riscos de interrupção dos serviços ou a possibilidade de alteração de servidores ou dados durante a sua execução deverá ser imediatamente interrompida. O Coren-SP (Conselho Regional de Enfermagem de São Paulo) será notificado de acordo com o plano de comunicação, para autorizar ou não a



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

continuidade dos testes.

**3.1.21.** O escopo do Pentest deve abranger os sistemas de negócios definidos, com o objetivo de identificar vulnerabilidades que poderiam permitir a um atacante influenciar um processo a ponto de comprometer a confiabilidade das atividades administrativas ou dos dados. Esses sistemas críticos serão escolhidos e comunicados pelo Coren-SP durante a reunião de alinhamento inicial.

**3.1.22.** A entrega dos resultados deve ser realizada por meio de relatório em formato descritivo e em planilha eletrônica. A entrega poderá ser realizada por meio de plataforma para realizar a gestão da correção das vulnerabilidades de forma centralizada e comprovar seu processo de governança para auditorias futuras.

**3.1.23.** A entrega dos resultados deve ser feita de forma segura, garantindo o sigilo do relatório.

**3.1.24.** A documentação dos resultados dos testes deve conter relação de endereços com as respectivas falhas e vulnerabilidades identificadas, bem como recomendações de plano de ação para a efetiva proteção da infraestrutura da CONTRATANTE.

**3.1.25.** Deverá ser entregue um Sumário Executivo;

**3.1.26.** Todas as atividades e tarefas deverão ser realizadas com base nas boas práticas nacionais e internacionais voltadas para a gestão e governança da tecnologia da informação e comunicação, definidas e sugeridas em modelos como a ITIL, a ISO 20.000, o COBIT, o PMBOK e a ISO 27.000.

**3.1.27.** Além destes, para a realização dos testes de intrusão deverão ser seguidas, obrigatoriamente, as orientações e técnicas constantes em ao menos uma das seguintes metodologias/padrões internacionais:

**3.1.27.1.** OSSTMM 3 (The Open Source Security Testing Methodology Manual);

**3.1.27.2.** OWASP TESTING GUIDE - The Open Web Application Security Project, em sua versão mais recente;

**3.1.27.3.** NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment); ou

**3.1.27.4.** PTES - Penetration Test Execution Standard.

**3.1.28.** As ferramentas utilizadas nos testes de intrusão são de responsabilidade da CONTRATADA, não devendo ser instaladas no ambiente tecnológico da CONTRATANTE. O processo de varredura deve ter um impacto mínimo sobre a rede. A utilização de ferramentas não deve integralizar a atuação do analista quando da realização do Pentest, sendo apenas auxiliares no processo de identificação, análise e posterior exploração de vulnerabilidades;

**3.1.29.** Os testes de intrusão deverão envolver, necessariamente, o uso de ferramentas específicas mais atualizadas e comumente utilizadas no mercado de segurança da informação, para tentar obter acesso não autorizado e privilegiado aos ativos de informações, simulando um ataque real. A CONTRATADA deverá utilizar ferramentas que atendam, no mínimo, as seguintes características:

**3.1.29.1.** Realize escaneamento utilizando base de dados atualizada com as



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

mais recentes ameaças e vulnerabilidades;

**3.1.29.2.** Faça avaliação de riscos com apresentação de score utilizando metodologia CVSS (Common Vulnerability Scoring System);

**3.1.29.3.** Apresente formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;

**3.1.29.4.** Deverá utilizar identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas;

**3.1.29.5.** As ferramentas deverão ser apresentadas para ciência, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades;

**3.1.29.6.** Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando as credenciais para se autenticar em sistemas Windows, UNIX ou qualquer ativo de infraestrutura, tais como dispositivos de rede, etc.n

**3.1.29.7.** Ser capaz de detectar, no mínimo, as vulnerabilidades elencadas no guia OWASP TOP 10 em sua versão mais atualizada;

**3.1.29.8.** Ser capaz de realizar “crawling/spidering” para descobertas de urls, hiperlinks, páginas, dentre outros.

**3.1.30.** Todos os custos envolvidos para a prestação dos serviços contratados correrão por conta da CONTRATADA, incluindo componentes de hardware ou de software não expressamente especificados e, contudo, se façam necessários para a plena execução dos serviços especificados neste Item.

### 3.2. TESTE DE ENGENHARIA SOCIAL

**3.2.1.** O serviço de engenharia social prestado pela CONTRATADA deve ser composto de no mínimo:

**3.2.1.1.** Entrega de relatório com todos os dados e aprendizados da campanha, de forma compilada e também detalhada para auxiliar na tomada de decisões e conscientização de usuários;

**3.2.1.2.** Construção e envio de e-mails para simulação do ataque de Phishing;

**3.2.1.3.** Relatório que permita avaliar se o usuário reportou à área de segurança o possível ataque de Phishing sofrido.

**3.2.2.** Todas as atividades da CONTRATADA que envolvam usuários do CONTRATANTE deverão ser realizadas em língua portuguesa, incluindo todos os níveis de atendimento, material fornecido, sites e conteúdos disponibilizados, pesquisas de satisfação, mensagens, entre outros.

**3.2.3.** As quantidades e os serviços específicos a serem executados nas campanhas de engenharia social serão definidos na reunião de planejamento, conforme demandado pela CONTRATANTE e conforme exemplos de engenharia social abaixo:

**3.2.3.1.** Envio de phishing ou spear phishing e seu devido controle de rastreamento de click;



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 3.2.3.2.** Uso de smishing, incluindo apps de comunicação, sms e voz em smartphone corporativo;
- 3.2.3.3.** Tailgating presencial em áreas restritas dentro do escopo autorizado;
- 3.2.3.4.** Candy Drop - teste do pendrive esquecido;
- 3.2.3.5.** Scareware ou ransomware falso, e seu devido controle de rastreamento de click;
- 3.2.3.6.** Demais técnicas inerentes à engenharia social.
- 3.2.4.** Esses serviços que necessariamente precisam ser realizados pessoalmente (como Tailgating e Candy Drop) serão feitos ao mesmo tempo nos seguintes moldes:
- 3.2.4.1.** Ao mesmo tempo e na mesma quantidade das campanhas de Pentest e Phishing;
- 3.2.4.2.** Serão testados 4 (quatro) andares/departamentos, como diretoria, fiscalização, atendimento, ou outros;
- 3.2.4.3.** Serão realizados apenas na sede em São Paulo;
- 3.2.4.4.** As definições de andares/departamentos mais precisamente serão feitas na reunião de planejamento;
- 3.2.4.5.** No mínimo 1 (um) pendrive por andar/departamento;
- 3.2.5.** O serviço deve possuir domínios personalizados de ataque prontos para sua simulação.
- 3.2.6.** A CONTRATADA deve possuir sua própria estrutura de envio de e-mails (Servidor SMTP), não onerando os recursos do Coren-SP para o envio dos e-mails de simulação.
- 3.2.7.** O serviço deve fornecer páginas de destino (landing page) em português e personalizadas para cada modelo de simulação, podendo serem elas uma revisão do phishing, uma página de erro, uma notificação sobre o programa de conscientização ou mesmo uma página personalizada de simulação de coleta de credenciais.
- 3.2.8.** O serviço deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos específicos.
- 3.2.9.** O serviço deve registrar a inserção de dados e demonstrar em relatório, na visão do usuário atacado, porém, esses dados não devem ser armazenados de nenhuma forma em bases internas da solução ou bases externas, fazendo apenas o registro de quais informações o usuário entregou no teste, não as informações em si;
- 3.2.10.** A CONTRATADA deve realizar a criação de templates personalizados de email para o Coren-SP, onde seja possível definir modelos por departamentos, em português e com a logo marca do Coren-SP, contendo no mínimo as seguintes opções:
- 3.2.10.1.** Customização do nome e extensão de um anexo do e-mail de simulação de ataque Phishing;
- 3.2.10.2.** Seleção de usuário e de grupo de usuários que farão parte da simulação;
- 3.2.10.3.** Seleção de agendamento com data e horário para início e fim de cada campanha, específica por grupo a ser atingido;
- 3.2.10.4.** Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing;
- 3.2.10.5.** Definição de assunto do e-mail de simulação do ataque Phishing;



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

- 3.2.10.6.** Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing;
- 3.2.11.** O serviço deve implementar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:
- 3.2.11.1.** Nome do usuário;
  - 3.2.11.2.** Sobrenome;
  - 3.2.11.3.** Endereço de e-mail;
  - 3.2.11.4.** Nome da empresa;
  - 3.2.11.5.** Dia, Data, Hora, Ano.
- 3.2.12.** A CONTRATADA deve disponibilizar treinamento em vídeo, palestra ou treinamento online para conscientização de todos os usuários, sobre os temas testados, ao final da campanha.
- 3.2.13.** A CONTRATADA deve, a pedido da CONTRATANTE, listar todos os e-mails de usuários que clicaram no phishing para que a CONTRATANTE possa enviar informativos direcionados.
- 3.2.14.** Após a primeira campanha, a entrega do serviço deve 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 do Coren-SP.
- 3.2.15.** O serviço, além de campanha de phishing, deve testar as ações dos usuários diante de dispositivos plugáveis desconhecidos que eles encontrarem (técnica chamada “Candy Drop”, “USB drop attack” ou “USB baiting”).
- 3.2.15.1.** No caso, todos os relatórios devem incluir, de forma discriminada, os dados obtidos nessa campanha.
- 3.2.16.** A CONTRATADA deve criar relatórios executivos e mostrar de forma gráfica no mínimo:
- 3.2.16.1.** Quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing;
  - 3.2.16.2.** Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;
  - 3.2.16.3.** Verificação de quantos usuários executaram o módulo de conscientização educacional Anti-Phishing;
- 3.2.17.** Deve apresentar de forma gráfica o resultado de qual grupo de usuários, departamento ou cargos mais caíram nos testes de simulação do ataque Phishing que foram envolvidos na simulação;
- 3.2.18.** Deve realizar a entrega dos dados/tabelas de todos os relatórios apresentados através de arquivo CSV editável ou similar.
- 3.2.19.** Deve disponibilizar relatórios avançados, executivos e de gestão, sobre as campanhas e resultados, no mínimo nos formatos pdf, pptx e xlsx.
- 3.2.20.** Deve permitir que se analise como os usuários estão se saindo de forma individualizada em comparação às outras empresas (Benchmarking).
- 3.2.21.** A CONTRATADA deverá manter a campanha em andamento por, no mínimo, 2 semanas



## CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

após o envio dos e-mails.

**3.2.22.** Os sistemas de segurança ativos devem ser ajustados pela CONTRATANTE, com informações de endereçamento passadas pela CONTRATADA, para não bloquear os e-mails da campanha de phishing, a fim de avaliar o grau de conscientização dos colaboradores.

**3.2.23.** A conclusão do projeto será compartilhada através de videoconferência, em um horário a ser agendado, apresentando um relatório que resuma as ações executadas, detalhes dos testes de phishing, recomendações de segurança e outras informações relevantes.

**3.2.24.** O cronograma para os testes de phishing seguirá o prazo de até 2 meses:

**3.2.24.1.** O cronograma estimado para o projeto engloba a fase de concepção dos testes de phishing, a execução, com duração mínima de uma semana para cada campanha, a consolidação dos dados obtidos, a elaboração e apresentação do relatório final, bem como a realização de uma palestra de conscientização.

**3.2.25.** As campanhas de teste de engenharia social e as quantidades de horas por campanha serão definidas de acordo com o tipo de teste e a quantidade de usuários que farão parte da amostra para o teste, conforme informado pela CONTRATANTE na reunião de planejamento;

**3.2.25.1.** Considerando que em abril de 2023 havia 558 usuários totais ativos no ambiente do Coren-SP;

**3.2.25.2.** Cada amostra será definida com uma quantidade mínima de usuários que seja capaz de representar o todo da gama de usuários em questão e assim, direcionar ações de melhoria do ambiente computacional e/ou conscientização dos colaboradores do Coren-SP.

Os resultados das campanhas serão compartilhados com a área de TI do Coren-SP, juntamente com consultoria que apresentará melhores práticas para aprimorar a conscientização dos colaboradores, além de abordar formas mais eficazes