ANEXO I

SERVIÇOS DE CIBERSEGURANÇA

1. GLOSSÁRIO

a) CSIRT: Time de Resposta a Incidentes de Segurança
b) Endpoint Baseline: Conformidade de Segurança em Endpoint
c) App Control Whitelist: Conformidade de Segurança e gerenciamento de software
d) Zero False Positive: Falsos positivos próximos a zero.
e) Tunning: Ajuste fino em configurações
f) ISO 27001: Padrão e Referência Internacional para Gestão da Segurança da informação
g) NDR: Network Detection and Response
h) Proxy: Desempenha a função de conexão do computador (local) à rede externa (Internet)
i) Dark Web: Parte obscura da internet, onde não existe regulação e, portanto, onde os crimes acontecem.
j) Deep Web: Zona da internet que não pode ser detectada facilmente pelos tradicionais motores de busca.
k) Endpoint: Qualquer dispositivo que se comunica diretamente à rede principal de conexão.
l) ZTNA: "Zero Trust Network Access" (Acesso à Rede de Confiança Zero), enfoca a verificação contínua da identidade e da segurança de qualquer entidade que tente acessar recursos de rede.
m) Terceiros: para este processo terceiros são empresas prestadoras de serviços ao Detran-PA.

2. CARACTERÍSTICAS INDIVIDUAIS DO SERVIÇO

2.1. SERVIÇO DE RESPOSTA A INCIDENTES (“CSIRT”)

2.1.1. REQUISITOS DE NEGÓCIO

a) O escopo de Serviço de Segurança Gerenciado deve fornecer um serviço totalmente gerenciado 24 horas por dia, 7 dias por semana, incluindo integridade e disponibilidade e gerenciamento completo de mudanças. Ele também deve fornecer acordos de nível de serviço estendidos (SLAs) e objetivos, incluindo configuração e ajuste de dispositivo.
b) A CONTRATANTE, quando julgar necessário, poderá solicitar atuação local DA CONTRATADA em suas dependências ou nas dependências de seus clientes.
c) Todos os custos de deslocamento serão de responsabilidade da CONTRATADA, sem qualquer ônus para a CONTRATANTE.
d) O Serviço de Segurança Gerenciado da CONTRATADA deverá seguir as melhores práticas da indústria para fornecer o cumprimento adequado e processos de gerenciamento de mudanças, eventos, incidentes e gerenciamento de problemas. Esses serviços garantem que os dispositivos de segurança estejam disponíveis e que a CONTRATANTE mantenha a conformidade com os requisitos regulamentares aplicáveis.
e) A CONTRATANTE busca serviço de Resposta a Incidentes, para reagir a incidentes relacionados a cibersegurança, assim trazendo resposta em tempo hábil para não trazer danos aos serviços prestados, aos dados e as aplicações.
f) O Serviço de Resposta a Incidentes (CSIRT) deve se integrar ao SOC entregue pela CONTRATADA no regime 24x7x365.
g) CONTRATANTE poderá solicitar a revisão sobre os resultados entregues na realização dos serviços que tenham sido feitos fora do escopo acordado no Contrato e/ou das normas, padrões, procedimentos e instruções técnicas da CONTRATANTE, ou ainda em desacordo com a legislação vigente, ficando a CONTRATADA obrigada a refazer o serviço conforme obrigação estabelecida neste Contrato, sem ônus para a CONTRATANTE.
h) Todo resultado entregue a partir dos serviços realizados pela CONTRATADA terá garantia de correções e

ajustes necessários durante os 90 (noventa) dias seguintes à conclusão daqueles serviços, mesmo que essa conclusão tenha ocorrido nos últimos 90 (noventa) dias do Contrato.
i) Dentro do período de garantia, a correção de erros nos serviços entregues pela CONTRATADA decorrente de incidentes provindos de segurança cibernética deverão ser efetuadas sem qualquer ônus para a CONTRATANTE, seja financeiro ou de atraso na prestação de outro(s) serviço(s), desde que, comprovadamente, não tenham se dado em razão das especificações feitas pela CONTRATANTE e/ou falta de estrutura para resolução, ou ainda pendência de renovações e/ou contratações.
j) Extinta a vigência do CONTRATO, a CONTRATADA terá 05 (cinco) dias úteis para atendimento.
k) Durante todo o período de execução dos serviços, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.
l) A CONTRATADA deve estar apta com conhecimento e ferramentas para recuperação dos principais ransomwares do mercado.

2.1.2. ELEMENTOS PRINCIPAIS DO SERVIÇO

2.1.2.1. Horário de Operação

a) Os Serviços Gerenciados de Segurança deverão fornecidos por meio de Centro de Operações de Segurança da CONTRATADA;
b) O horário de funcionamento do serviço é de 24 horas por dia, 7 dias por semana;

2.1.3. COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

O serviço deverá ser prestado por meio de CSIRT da CONTRATADA

2.1.3.1. Matriz de Serviços

A CONTRATADA deve fornecer um conjunto central de módulos de serviço e elementos de serviço associados.

Módulos e Elementos de Serviço
Elementos de serviços principais
24 x 7 Horas de Operação
Centros de Operações de Segurança
Portal Web para CONTRATANTE
Suporte ao idioma
Gerenciamento de Dispositivos
Comunicações
Gestão de Escalonamento
Recursos de gerenciamento de dispositivos
Módulos e Elementos de Serviço
Saúde e Disponibilidade
Monitoramento de Saúde e Disponibilidade
Melhoria e Recomendação de Saúde e Disponibilidade
Implementação de mudanças de saúde e disponibilidade
Gerenciamento de Incidentes
Geração de Incidentes
Diagnóstico de Incidente

Resolução de Incidentes
Relatórios de Incidentes
Gestão de Capacidades
Monitoramento e relatórios de capacidade
Recomendação de melhoria de capacidade
Planejamento de Capacidade
Implementação de mudança de capacidade
Rastreamento e relatórios de ativos
Controle de itens de configuração e atualizações
Relatório de status do item de configuração
Cumprimento de solicitação de serviço
Gerenciamento de solicitações de serviço
Gestão de Mudanças
Gerenciamento de Problemas
Identificação e Registro de Problemas
Relatórios de problemas
Identificação de Soluções
Implementação de soluções

TABELA MATRIZ DE SERVIÇOS

2.1.3.2. REQUISITOS DE SERVIÇO

2.1.3.2.1. Em todos os casos

O modelo de entrega padrão deve ser 24 horas por dia, 7 dias por semana, usando o SOC da CONTRATADA.

2.1.3.2.2. Item de configuração

O serviço deverá gerenciar todos os itens de configuração suportados, definidos neste termo de referência.

2.1.3.3.3. Contatos de segurança designados

A CONTRATANTE fornecerá dois membros da equipe para serem contatos de segurança e um contato de Service Desk para interagir com os serviços de gerenciamento de dispositivos.

2.1.3.4. Requisitos de Comunicação

2.1.3.4.1. Acesso

Os serviços gerenciados de segurança exigem um acesso remoto seguro.

2.1.3.4.2. Conectividade – Serviços Gerenciados

a) A CONTRATANTE fornecerá, em tempo de transição, a lista de dispositivos a serem monitorados.
b) A CONTRATANTE será responsável pela configuração SNMP nos equipamentos definidos na lista de dispositivos a serem monitorados, para obtenção de estatísticas.
c) A CONTRATANTE será responsável por fornecer a topologia da rede para facilitar no entendimento do todo e na sugestão de alterações de desenho e melhorias.

2.1.3.5. Elementos de serviço principais

2.1.3.5.1. Horas de Operação

Os Serviços de Gerenciados de Segurança deverão ser entregues através dos SOC (Security Operations Center, centro de operações de segurança) da CONTRATADA. A menos que seja declarado o contrário, as horas de operação deverão ser 24 horas por dia, 7 dias por semana.

2.1.3.5.2. Centros de Operação de Segurança

A CONTRATADA deverá prestar serviços através de SOC's próprios.

2.1.3.5.3. ITSM

A CONTRATADA deverá prover uma interface para ITSM, que é um aplicativo baseado na Web disponível globalmente, que permitirá que os usuários da CONTRATANTE interajam, gerenciem e monitorem os Serviços gerenciados de segurança.

2.1.3.5.4. Suporte ao idioma

Os serviços deverão ser prestados em português do Brasil, a menos que haja acordo prévio e aprovação da CONTRATANTE.

2.1.3.5.5. Gestão

a) O gerenciamento deverá ser fornecido como um componente central da oferta de serviços gerenciados de segurança, onde a CONTRATANTE fornecerá a CONTRATADA um acesso privilegiado aos itens de configuração dentro do escopo.
b) A CONTRATADA deverá criar uma conta de administrador (Break Glass account) para a CONTRATANTE e armazenará com segurança as credenciais e senha. No caso de uma emergência em que a CONTRATADA não consiga fazer uma alteração ou acessar a infraestrutura de configuração item/gerenciamento, o contato de segurança principal da CONTRATANTE deverá ser fornecido com as credenciais e senha.
c) Cada vez que a CONTRATANTE usar a conta Break Glass, a CONTRATADA deverá redefinir a conta com uma nova senha.

2.1.3.5.6. Comunicações Infraestrutura do Serviço Gerenciado de Segurança

A CONTRATADA deverá utilizar uma infraestrutura regional com segurança incorporada por princípios de design. Deverá ser altamente resiliente e protegida e reconhecida pelo uso do melhor de metodologias, práticas, ferramentas e técnicas.

2.1.3.5.7. Notificações

2.1.3.5.7.1. Email

a) Para comunicação escrita, deverá ser utilizada a plataforma de comunicação da CONTRATANTE, sendo que o e-mail regular poderá ser utilizado como segunda opção, em regime de contingência.
b) Por razões de segurança e privacidade de dados, as notificações deverão conter apenas informações mínimas para notificar a CONTRATANTE sobre a criação ou atualizações de casos. Essas notificações não devem conter nenhuma informação sensível além do número de referência do ticket apropriado (e, quando possível, não divulgar qualquer informação privada na breve descrição do ticket).
c) A CONTRATANTE poderá enviar mensagens relacionadas a casos novos ou existentes para CONTRATADA. No caso de nenhum número de referência for fornecido, a CONTRATADA deverá criar um caso com uma

descrição curta com base na linha de assunto fornecida.

2.1.3.5.7.2. Anexos de arquivos

Diagramas, imagens, PDF's, executáveis e quaisquer outros anexos não deverão ser anexados a nenhum caso por e-mail. Quando os anexos de arquivos forem necessários, a CONTRATANTE fará através de seu navegador web conectado ao Portal.

2.1.3.5.7.3. Telefone

A equipe da CONTRATADA poderá entrar em contato com a CONTRATANTE e a CONTRATANTE pode entrar em contato equipe da CONTRATADA por telefone.
Em ambos os casos, uma autenticação deverá ser completada para verificar a identidade da CONTRATANTE.

2.1.3.5.7.4. Portal ITSM da CONTRATADA

Salvo declaração e acordo em contrário, todas as outras comunicações originárias da equipe da CONTRATADA deverão ser seguras, seguindo as melhores práticas de segurança e serão através do Portal Web da CONTRATADA.

2.1.3.5.8. Monitoração Protocolos

Os itens de configuração da CONTRATANTE devem ser monitorados utilizando vários protocolos, incluindo Simple Network Management Protocol (SNMP) v2, v3, Secure Shell (SSH) v2, Hypertext Transfer Protocol Secure (HTTPS) e Internet Control Message Protocol (ICMP).

2.1.3.5.8.1. Eventos de monitoramento de saúde e disponibilidade

Os feeds de eventos a partir de itens de configuração no escopo deverão ser enviados com segurança para o servidor de monitoramento através de uma ferramenta de gestão de acessos críticos, sendo a VPN uma opção de contingência.

2.1.3.5.9. Engenharia Acesso ao item de configuração

O acesso à linha de comando deverá ser protegido via SSH v2. A ferramenta de gestão de acessos críticos oferecerá um jump-server da CONTRATADA confiável dentro da infraestrutura DE SERVIÇO GERENCIADO DE SEGURANÇA, deverá ser estabelecido para fornecer acesso SSH.

2.1.3.5.10. Gestão de Escalonamento

a) A CONTRATADA deverá fornecer um processo de escalonamento e definição de responsabilidades para abordar questões de escala. Para escalar um caso, a CONTRATANTE poderá telefonar ou enviar um e-mail para o service desk (citando o número de referência).
b) A CONTRATADA poderá rebaixar um caso escalonado, se ele estiver sendo tratado dentro de um prazo ou resolução programada foi fornecida a CONTRATANTE e em processo de teste. Para escalonamentos iniciados pela CONTRATADA, deverá ser obtida a aprovação da CONTRATANTE antes de rebaixar um incidente de Segurança escalonado, solicitação de mudança ou solicitação de serviço.
c) Se for dada justificativa suficiente, a CONTRATANTE poderá solicitar que seu caso seja escalonado para uma prioridade maior a qualquer momento. Após a reversão, o gerente do SOC deverá ser responsável por concordar com as ações.
d) Também é necessário a CONTRATANTE fornecer uma lista de escala para caso de identificação de incidente

grave e a primeira linha de contato não responda, e assim sucessivamente até que ou se chegue ao topo da lista ou que seja atendido para evitar um dano maior ao ambiente.

2.1.3.5.11. Recursos de gerenciamento de dispositivos

2.1.3.5.11.1. Monitoramento de Saúde e Disponibilidade

O serviço gerenciado de segurança deverá monitorar os principais indicadores de desempenho do estado de serviço e utilização de recursos do item de configuração no escopo para determinar a saúde, o desempenho e a disponibilidade em geral. O serviço deverá gerar automaticamente incidentes no sistema com base nos eventos, que excedem os limites em relação aos thresholds estabelecidos. O engenheiro do Serviço Gerenciado de Segurança da CONTRATADA deverá investigar e analisar os eventos para determinar uma possível ação corretiva ou de controle para resolver o incidente relacionado, bem como, em caso de falso positivo revisitar a regra a fim de adequar melhor para o ambiente da CONTRATANTE.

2.1.3.5.11.2. Melhoria e Recomendação de Saúde e Disponibilidade

a) A CONTRATADA deverá utilizar ciclos e limiares de pesquisa padrão ao monitorar itens de configuração no escopo. A CONTRATADA deverá ajustar os limiares com base nos dados históricos coletados para eliminar eventos desnecessários que ocorrem. Com esses dados, deverá identificar métodos potenciais para melhorar o desempenho do item de configuração e a saúde e a disponibilidade em geral.

b) A CONTRATANTE também poderá solicitar a personalização de limites através de processos de gerenciamento de mudança padrão.

2.1.3.5.11.3. Implementação de mudanças de saúde e disponibilidade

Se um item de configuração exigir alterações, a CONTRATADA seguirá o processo padrão de gerenciamento de alterações descrito na seção Gerenciamento de Gestão de Mudanças.

2.1.3.5.11.4. Gerenciamento de Incidentes

O Gerenciamento de Incidentes se concentrará em responder a qualquer interrupção não planejada na operação de itens de serviço e configuração para minimizar qualquer impacto nas operações de negócios e garantir a qualidade e a disponibilidade do serviço.

2.1.3.5.11.5. Geração de Incidentes

a) Os incidentes podem ser gerados através do Monitoramento de Saúde e Disponibilidade pelo SOC ou CONTRATANTE abrindo um caso de Incidente através do Portal ou chamada telefônica para o CSIRT.

b) Após um caso de incidente ser criado através do Portal, com um Impacto e Urgência fornecidos, a equipe do CSIRT validará o ticket e modificará o Impacto e a Urgência, conforme necessário.

c) Para um caso de incidente levantado através de uma chamada telefônica para o CSIRT, o CSIRT deverá criar um caso de incidente em nome da CONTRATANTE com o impacto e urgência relevantes.

2.1.3.5.11.6. Diagnóstico de Incidente

a) Os casos de incidente deverão ser gerenciados com base na prioridade do ticket de incidente levantado no Portal. As prioridades deverão ser calculadas com base no impacto e Urgência de um caso de incidente. As prioridades deverão ser definidas como Crítico, Alto, Média e Baixo, conforme descrito na tabela abaixo.

		URGÊNCIA		
		1. Trabalho bloqueado	2. Trabalho degradado	3. Trabalho não afetado
IMPACTO	Toda a organização	Crítico	Crítico	Alto
	Vários departamentos	Crítico	Alto	Médio
	Departamento único	Alto	Médio	Baixo
	Individual	Médio	Baixo	Baixo

TABELA MATRIZ IMPACTO - URGÊNCIA DE SERVIÇOS

b) O CSIRT deverá realizar a triagem do incidente para avaliar a prioridade.
c) Incidentes deverão ser atribuídos ao engenheiro SOC apropriado para investigação e análise mais aprofundada para identificar um plano de correção para resolver o caso do incidente.
d) Por meio do portal, a CONTRATANTE deverá ser notificada de atualizações de um incidente e qualquer plano de restauração para resolver o caso.

2.1.3.5.11.7. Resolução de Incidentes
a) A CONTRATADA deverá trabalhar para resolver os incidentes e movê-los para um estado resolvido no Portal de para permitir que a CONTRATANTE confirme a resolução. Relatórios de Incidentes.
b) A CONTRATANTE deverá ser notificada de todos os incidentes por meio de uma plataforma de comunicação segura, sendo o e-mail uma opção de contingência, para notificação, que conterá informações mínimas para fins de segurança, com os detalhes completos do incidente disponíveis apenas através do Portal.

2.1.3.5.11.8. Monitoramento e relatórios de capacidade
a) Os sistemas de monitoramento utilizados no serviço de Gerenciamento de Dispositivos deverão verificar regularmente vários pontos de telemetria. Através do monitoramento continuo, deverá ser possível destacar tendências potencialmente impactantes. Isso deverá ser utilizado para determinar se há um problema que precisa ser resolvido ou se os itens de configuração estão se tornando sobrecarregados demais, por exemplo, um preenchimento de disco com dados de log. Usando isso como ponto de partida para gerenciamento de incidentes ou problemas, a CONTRATADA trabalhará com a CONTRATANTE para aconselhar sobre resolução potencial ou mitigar o risco.
b) A CONTRATADA deverá utilizar limites padrão ao coletar dados de monitoramento. Reconhecemos que esses limites podem não ser aplicáveis a alguns ambientes da CONTRATANTE, a CONTRATADA deverá trabalhar com a CONTRATANTE para ajustar os limites durante o processo de Transição de Serviço ou após a entrada do serviço, onde uma linha de base poderá ser identificada.
c) Recomendação de melhoria de capacidade.
d) Quando o monitoramento da CONTRATADA determinar que um dispositivo está sobrecarregado, deverá entrar em contato com a CONTRATANTE para determinar o melhor plano e caminho a seguir. Exemplos incluem, mas não se limitam ao seguinte:
e) Solicitar a CONTRATANTE que altere os níveis de registro ou a arquitetura de rede.
f) Solicitar a CONTRATANTE que altere os níveis de monitoramento dentro do item de configuração (por exemplo, desligar o registro de depuração)
g) Solicitar a CONTRATANTE a atualização de hardware ou licenças para facilitar maior capacidade.

2.1.3.5.11.9. Planejamento de Capacidade
Com os dados de tendência acima mencionados disponíveis, CONTRATADA, Parceiros e/ou CONTRATANTE poderão tomar decisões sobre requisitos futuros e crescimento esperado. Isso fornecerá um planejamento avançado inestimável para os responsáveis pelo orçamento ou planejamento de capacidade. Por exemplo, relatórios de análise de tendências mostrarão o consumo de disco ao longo do tempo, o que pode ser um indicador da necessidade de obter novos hardwares ou armazenamento adicional no próximo ciclo de orçamento.

2.1.3.5.11.10. Rastreamento e relatórios de ativos Gravação de itens de configuração
Através da medição consistente e uniforme da telemetria a partir de itens de configuração de segurança gerenciados, a CONTRATADA deverá fazer recomendações ou levantar um ticket para mudança a ser aprovado pela CONTRATANTE para melhorar ou evitar problemas futuros de capacidade que possam surgir. Isso está sujeito a aprovações necessárias e os conselhos que estão sendo seguidos. Quaisquer problemas de capacidade relacionados à atualização ou design de hardware não estão no escopo deste serviço.

2.1.3.5.11.11. Rastreamento e relatórios de ativos Gravação de itens de configuração
A CONTRATADA deverá registrar e rastrear itens de configuração da CONTRATANTE no escopo com informações disponíveis no Portal.

2.1.3.5.11.12. Principais atualizações de versão
a) As principais atualizações de versão requerem planejamento cuidadoso, coordenação, gerenciamento e planejamento de reversão. A CONTRATADA deverá considerar todas as principais atualizações de versão como de alto risco no que diz respeito aos ambientes de produção da CONTRATANTE e serão tratadas pontualmente.
b) Sempre que aplicável, os bancos de dados de assinatura de itens de configuração que geralmente deverão ser automatizados e requerem conectividade entre o item de configuração e a Internet para baixar as atualizações, deverão ser verificados se as atualizações de assinaturas estão sendo atualizadas com sucesso.

2.1.3.5.11.13. Falhas de assinatura
Se a atualização de assinatura falhar, um incidente deverá ser levantado em nome da CONTRATANTE. Posteriormente, quaisquer erros relacionados à capacidade de um item de configuração de atualizar as assinaturas deverão ser resolvidos usando o processo padrão de gerenciamento de incidentes da CONTRATADA.

2.1.3.5.11.14. Escalonamentos de assinaturas
Se a causa da incapacidade do item de configuração de atualizar assinaturas for um erro ou deficiência no banco de dados do fabricante, a CONTRATANTE deverá escalar o problema para o fabricante e/ou fornecedor.

2.1.3.5.11.15. Responsabilidades da CONTRATANTE de Assinatura
A CONTRATANTE é responsável pela compatibilidade, teste de aceitação do usuário e testes funcionais dentro do ambiente de produção da CONTRATANTE. A CONTRATANTE garante que todos os itens de configuração estejam conectados à internet para permitir a entrega de atualizações automatizadas de assinatura do fabricante de itens de configuração, diretamente através de um proxy ou através de um sistema de gerenciamento dedicado, sempre que aplicável.

2.1.3.5.11.16. Assinatura - Contrato de nível de serviço implícito
Se a falha de um mecanismo de atualização de assinatura for diagnosticada como um incidente relacionado ao

fabricante, o nível de serviço para resolver o incidente estará de acordo com o contrato de fornecedor de terceiros do fabricante.

2.1.3.5.11.17. Backup de itens de configuração

a) A CONTRATADA deverá manter um backup do sistema de itens de configuração e configuração no escopo em caso de falha. A ferramenta a ser considerada deve levar em consideração sua compatibilidade com o ambiente do DETRAN-PA.

b) Antes de implementar uma solicitação de alteração, a CONTRATADA deverá aplicar um backup de configuração e utilizar para reverter para a última configuração conhecida, no caso de uma falha ou de uma solicitação da CONTRATANTE.

c) A CONTRATADA deverá fazer backup das seguintes informações do item de configuração (quando aplicável):

1. Configuração do sistema (SO e configuração)
2. Regras de configuração
3. Configuração de assinatura
4. Arquivos de configuração
5. Cumprimento de solicitação de serviço

d) A CONTRATADA deve realizar o cumprimento do serviço, que se concentra na solicitação de informações, conselhos ou acesso.

e) A título de verificação, a CONTRATADA deverá gerar eventos periódicos de testes de restauração de backup e relatórios ao time de gestão da CONTRATANTE, como garantia de melhores práticas.

2.1.3.5.11.18. Gerenciamento de solicitações de serviço

As solicitações de serviço deverão ser gerenciadas através do processo ITIL e deverão ser levantadas através de um caso no Portal. A CONTRATADA rastreará, monitorará e relatará a obtenção de várias métricas de desempenho importantes mensalmente.

2.1.3.5.11.19. Solicitação de Informações

A CONTRATANTE poderá solicitar informações sobre o desempenho, configuração ou outros aspectos dos itens de configuração no escopo através do Portal. A CONTRATADA deverá fornecer as informações na Solicitação de Serviço.

2.1.3.5.11.20. Relatórios de solicitação de serviço

Todos os incidentes, solicitações de serviço ou problemas deverão ser registrados no sistema e reportados através do Portal.

2.1.3.5.11.21. Gestão de Mudanças

A pedido da CONTRATANTE, a CONTRATADA deverá implementar uma solicitação de alteração para itens de configuração no escopo de acordo com uma tarefa associada a um catálogo ou tarefa não padrão.

2.1.3.5.11.22. Solicitações de origem da CONTRATANTE

Os contatos da CONTRATANTE válidos devem enviar uma solicitação para caso de mudança dentro do Portal.

2.1.3.5.11.23. Solicitações de origem CONTRATADA

A CONTRATADA poderá enviar um pedido para caso de mudança quando uma mudança de controle correta

é necessária para resolver um problema ou incidente.

2.1.3.5.11.24. Relatórios de mudanças

a) Deverão sempre utilizar o Portal para informar e acompanhar todas as alterações.

b) A parte que faz uma mudança precisa abrir um pedido aplicável de mudança no Portal antes da implementação para garantir a coordenação entre ambas as partes.

2.1.3.5.11.25. Solicitação de Mudança

a) Todos os pedidos de tipos de alteração deverão seguir o processo de Gerenciamento de Mudanças e requerem aprovação da CONTRATADA. As tarefas deverão ser derivadas por tecnologia, o que corresponde ao número de Unidades Service utilizadas por cada tarefa.

b) A CONTRATANTE emprega 3 (três) tipos de solicitação de mudança. Deverão ser elas:

1. Mudança Normal, alterações normais requerem aprovação (tanto de CONTRATADA quanta CONTRATANTE, respectivamente) antes de serem implementadas. Nem a CONTRATANTE nem a CONTRATADA estão autorizados a aplicar alterações em nome do outro sem o consentimento documentado de indivíduos autorizados (documentados dentro de um Grupo de Aprovação de mudanças no Portal) de ambas as partes através de um pedido de alteração no Portal.
2. Mudança Padrão, quando um ticket de mudança padrão for criado através do Portal, a CONTRATADA é autorizada pela CONTRATANTE a aplicar mudanças sem solicitar autorização. No entanto, o processo de aprovação interno da CONTRATADA ainda será válido.
3. Mudanças de emergência, uma mudança de emergência é considerada um pedido de mudança que deve ser implementado o mais rápido possível, por exemplo, para resolver um incidente ou para implementar um patch de segurança. A CONTRATADA trabalhará com a CONTRATANTE durante o processo de Gerenciamento de Mudanças.

2.1.3.5.11.26. Cancelando um pedido de mudança

a) A CONTRATANTE poderá cancelar uma solicitação até 2 horas antes de qualquer alteração programada estar comprometida com configuração do dispositivo.

b) Se a CONTRATANTE quiser reverter uma mudança que já foi implementada, a CONTRATANTE enviará uma nova solicitação de serviço para alteração através do Portal.

2.1.3.5.11.27. Implementação de Mudanças

a) A parte que faz a mudança deve concluir e documentar as seguintes tarefas associadas a cada alteração:

1. Fazer backup da configuração de execução atual antes de alterar.
2. Garantir que uma cópia de qualquer software e/ou firmware aplicável esteja prontamente acessível.
3. Garantir que um plano de reversão esteja documentado se há problemas com a mudança.
4. Atribuir um número de ticket interno (se aplicável) para acompanhar a mudança para fins de auditoria.
5. Implementar e testar a mudança (na medida do possível – a responsabilidade de teste também é compartilhada com a CONTRATANTE) para confirmar se a mudança atendeu aos requerimentos conforme especificado pelo requisitante.
6. Criar um backup da nova configuração após a implementação da mudança.
7. Atualizar o ticket de solicitação de serviço da CONTRATADA indicando se a mudança foi bem-sucedida ou não.
8. É imperativo que cada mudança esteja totalmente documentada dentro do Portal para garantir que a CONTRATADA ou a CONTRATANTE possam rapidamente solucionar problemas quando ocorrerem consequências negativas inesperadas.

2.1.3.5.11.28. Exceções

A CONTRATANTE entende que quaisquer exceções que possam surgir devido ao desvio ou tentativa de contornar os processos descritos aqui podem resultar em uma configuração(s) instável e/ou não compatível.

2.1.3.5.11.29. Responsabilidades da CONTRATADA

Revisar o incidente, solicitações de serviço e qualquer documentação sobre as mudanças realizadas pela CONTRATANTE e buscar esclarecimentos sempre que necessário.

2.3.1.5.11.30. Análise de impacto de mudança

a) Como parte do processo de projeto de mudança, a CONTRATADA deverá realizar uma análise de impacto de mudança de acordo com todos os pedidos de casos de mudança (pré e/ou pós- implementação). A análise é realizada antes da implementação de qualquer solicitação de caso de alteração, para garantir:

1. Hardware/software atende a todos os pré-requisitos
2. Existem backups da versão/configuração anterior
3. Qualquer alteração é consistente com as melhores práticas de segurança e não compromete a rede, o serviço ou da CONTRATADA ou da CONTRATANTE.
4. Qualquer alteração é relevante para o ambiente da CONTRATANTE
5. Qualquer alteração pode ser implementada dentro do prazo solicitado

b) A CONTRATADA deverá considerar a Análise de Impacto de Alteração completa quando a CONTRATANTE abordar todas as questões levantadas durante a análise (se aplicável), e o engenheiro reconhecer o recebimento de um ticket válido para mudança através do Portal.

2.1.3.5.11.31. Gerenciamento de Problemas

2.1.3.5.11.31.1. Identificação e Registro de Problemas

A CONTRATADA deverá seguir as melhores práticas da ITIL para identificação e registro de problemas. A identificação de problemas será realizada de várias maneiras e normalmente resultará em um caso de problema na ferramenta ITSM e no Portal. Normalmente, os problemas deverão ser derivados de uma série de fatores, tais como:

1. Incidentes repetidos de mesma ou similaridade dentro de uma única localidade ou em várias localidades.
2. Problemas compostos causados por múltiplos incidentes de natureza diferente dentro de uma única localidade.

2.1.3.5.11.31.2. Notificação de Problema de Fabricante em dispositivo do CONTRATANTE

a) Falta de patch oportuno do Fabricante para resolver uma vulnerabilidade de segurança.
b) Análise de tendências.
c) Relatórios de problemas.
d) Todos os problemas deverão ser registrados no sistema ITSM e reportados através do Portal.
e) Identificação e gravação de soluções.
f) Uma vez identificado e registrado um problema, um plano sugerido ou uma série de opções sugeridas para resolução deverão ser registradas no ticket do problema, quando apropriado.

2.1.3.5.11.31.3. Implementação das Alternativas Apuradas

A CONTRATANTE e a CONTRATADA discutirão e concordarão com a melhor ou mais adequada alternativa, com a CONTRATANTE sendo responsável por implementar como uma mudança controlada ou uma série de mudanças em consonância com o seu processo de mudança padrão.

2.1.3.5.12. SERVICE LEVEL AGREEMENTS

Categoria	Descrição	Prioridade	SLA	Penalidades	Limite de Penalidade	Horário de Serviço
Solicitação de serviço	A CONTRATADA Atribuirá uma Solicitação de Serviço com prioridade após o recebimento do tíquete no Service Desk da CONTRATADA	P1 e P2	15 MINS	1% da taxa de serviço mensal	Até 5% do valor total do contrato ao longo dos 15 meses	24/7
		P3 & P4	4 HRS			
Solicitação resolvida	A CONTRATADA resolverá uma Solicitação de Serviço com prioridade _ dentro de _ minutos após o recebimento do tiquete no Service Desk da CONTRATADA	P1	2 dias corridos	1% da taxa de serviço mensal	Até 5% do valor total do contrato ao longo dos 15 meses	24/7
		P2 & P3	5 dias corridos			
		P4	10 dias corridos			
Incident Management – Response	A CONTRATADA atribuirá um tíquete de Incidente com prioridade após o recebimento do tíquete no Service Desk da CONTRATADA	P1 & P2	30 Min	1% da taxa de serviço mensal	Até 5% do valor total do contrato ao longo dos 15 meses	24/7
		P3 & P4	60 Min			
Incident Management – Resolve	A CONTRATADA resolverá um incidente com prioridade após o recebimento do tíquete na Equipe de Gerenciamento de Dispositivos da CONTRATADA	P1	8 Hrs	N/A	N/A	24/7
		P2	16 Hrs			
		P3 & P4	48 Hrs			
Emergency Change Response	A CONTRATADA atribuirá um tíquete de Mudança de Emergência após o recebimento do tiquete no Service Desk da CONTRATADA	N/A	60 Min	N/A	N/A	24/7
Change Response	A CONTRATADA atribuirá um tíquete de Mudança após o recebimento do tiquete no Service Desk da CONTRATADA	N/A	60 Min	N/A	N/A	24/7

Change Implementation – Complete	A CONTRATADA Completará as alterações antes do final da janela de alteração, conforme acordado mutuamente entre o CONTRATANTE e a CONTRATADA	N/A	95%	N/A	N/A	24/7
Resolve Notification (Service Level Objective) – Notify	A CONTRATADA fornecerá uma notificação de resolução para cada tíquete de após a restauração do serviço.	N/A	30 Min	N/A	N/A	24/7
Elaboração de documentos de GMUD envolvendo os ativos de segurança da CONTRATADA	A CONTRATADA irá elaborar documentos de mudança que envolvam os ativos gerenciados por seu serviço de segurança gerenciado	N/A	2 dias corridos			8/5
Planejamento e implantação de Novas ferramentas e/ou funcionalidades no ambiente de segurança da CONTRATADA	A CONTRATADA irá analisar, junto com a CONTRATANTE, o planejamento e o esforço necessário para implantação ou adição de funcionalidades presentes nas ferramentas e no escopo de soluções descrito neste Termo de Referência	N/A	7 dias corridos			8/5
Análise de potencial ameaças demandadas por usuários e/ou time de segurança da Informação	A CONTRATADA fará Threat Hunting e análise sobre ameaças demandadas por usuários ou pelo time de segurança da informação da CONTRATANTE	N/A	1 dia corrido			8/5

TABELA SERVICE LEVEL AGREEMENTS

2.1.4. ESCOPO DA OPERAÇÃO DO SERVIÇO

A CONTRATADA deverá prover, dentro dos serviços de CSIRT, serviço de resposta a incidentes identificados e reportados. Abaixo, são especificados o escopo de serviços requeridos pela CONTRATANTE:

1. Aceitação de Bilhete de Incidente de Segurança da Informação
2. Análise de incidentes de segurança da informação

3. Triagem de incidentes de segurança da informação (priorização e categorização)
4. Coleta de informações
5. Coordenação de análise detalhada
6. Análise da causa raiz de incidentes de segurança da informação
7. Correlação de incidente cruzado
8. Análise de artefatos e evidências forenses
9. Análise de mídia ou superfície
10. Engenharia reversa
11. Tempo de execução e / ou análise dinâmica
12. Análise comparativa
13. Mitigação e recuperação
14. Plano de resposta estabelecido
15. Medidas ad hoc e contenção
16. Restauração de sistemas
17. Suporte de outras entidades de segurança da informação
18. Coordenação de incidentes de segurança da informação
19. Comunicação Interna
20. Distribuição de notificação interna
21. Distribuição interna de informações relevantes
22. Coordenação de atividades
23. Relatórios Internos
24. Apoio à gestão de crises
25. Distribuição de informações aos constituintes
26. Relatório de status de segurança da informação
27. Comunicação de decisões estratégicas

2.2. SERVIÇO ESPECIALIZADO EM GERENCIAMENTO DE VULNERABILIDADES E GESTÃO DE PATCHES

2.2.1. REQUISITOS DE NEGÓCIO

a) O serviço de Gerenciamento de Vulnerabilidades e gestão de patches incluirá o suporte e análise dispositivos localizados on premises e em Cloud utilizando coletores e Scan de Vulnerabilidades locais.
b) O serviço de Gerenciamento de Vulnerabilidades, deverá efetuar a gestão de Patchs Virtuais (Virtual Patching), mostrando necessidade e oportunidades de atualização baseados em vulnerabilidades de versões atualmente utilizadas.
c) A contratada obrigatoriamente deverá apoiar a execução de atualização dos patchs a fim de garantir que a atualização sanou a vulnerabilidade previamente apontada.
d) A CONTRATADA deve fornecer o serviço por meio de um Centro de Operações de Segurança (SOC) próprio.
e) O serviço deve permitir a implantação de um procedimento de investigação e busca por ameaças no ambiente da CONTRATANTE.
f) Uso de metadados para detecção e investigação de ameaças.
g) O objetivo é identificar comportamentos maliciosos mais complexos.
h) Analistas de segurança devem poder elaborar consultas personalizadas a partir dos resultados anteriores para identificar comportamentos maliciosos sofisticados.
i) Deve permitir a alimentação do serviço com múltiplas fontes de inteligência de ameaças.

j) Isso inclui pesquisas internas, fontes comerciais, comunidades Open Source e entidades especializadas de setores específicos.
k) O serviço deve ser escalonável para lidar com o grande volume de dados coletados, processados e armazenados.
l) O desempenho do serviço deve ser garantido mesmo diante de um alto fluxo de informações.

2.2.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) O serviço deve ser em nuvem – SaaS
b) O serviço deve ter visibilidade e cobertura em tempo real para os sistemas operacionais e aplicativos web da organização.
c) O serviço deve fornecer uma solução integrada para gerenciamento de vulnerabilidade, priorização de risco e remediação em uma única plataforma.
d) O serviço deve rodar em uma das três nuvens mais utilizadas.
e) O serviço deve funcionar e suportar os serviços e aplicações instalados no Sistema Operacional.
f) Modelo de risco personalizável.
g) Avaliação contínua de vulnerabilidades.
h) Reconhecimento automático de aplicativos.
i) Priorização de ameaças com base em ativos.
j) Priorização de vulnerabilidade combinada com inteligência interna.
k) Priorização e remediação de vulnerabilidade do início ao fim.
l) Processo de classificação de risco para priorizar a correção de vulnerabilidades descobertas.
m) Classificação de risco baseada em ativos.
n) Classificação de risco por aplicativos.
o) Deve apresentar a classificação de risco e priorizar as vulnerabilidades a serem corrigidas em ordem de criticidade não só do CVE, mas também em relação à um contexto de performance e situação do ambiente.
p) Mapeamento de priorização.
q) Gerenciamento de patches para o sistema operacional Windows.
r) Gerenciamento de patches para aplicativos de terceiros no Windows
s) Gerenciamento de patch para Linux OS.
t) Gerenciamento de patches para aplicativos de terceiros no Linux.
u) Detecção de vulnerabilidades em tempo real.
v) Parar a exploração de software em tempo real.
w) Informações legadas de CVE.
x) Atualização diária de vulnerabilidades.
y) Deve suportar um número de vulnerabilidades legadas igual ou superior a 140.000.
z) Deve fazer scan de vulnerabilidade e identificar patches em sistemas operacionais.

2.2.3. REQUISITOS DE SERVIÇO

a) A CONTRATANTE espera que a CONTRATADA entregue este serviço para o SOC 24 horas por dia, 7 dias por semana.
b) A detecção, análise e relatórios detalhados de incidentes de segurança de ataques cibernéticos devem ser fornecidos por meio de uma combinação de serviços da CONTRATADA.
c) A CONTRATADA deve fornecer toda solução tecnológica e serviço necessário para execução do serviço.
d) A CONTRATANTE deverá possuir e disponibilizar estrutura central para visualização de todas as vulnerabilidades e status das aplicações dos patchs.
e) A CONTRATADA deve fornecer toda solução tecnológica e serviço necessário para execução do serviço de

gestão de vulnerabilidade e aplicação de patchs.
f) A CONTRATADA deverá disponibilidade painel para a CONTRATANTE gerenciar algumas atualizações, quando achar necessário.
g) A CONTRATADA deverá testar os patchs críticos antes de aplicar no ambiente da CONTRATANTE.
h) A CONTRATADA deverá instalar um número ilimitado de patches de software qualificados e aplicáveis e atualizações de versão menor do Sistema Operacional (OS) para os itens do escopo. Todos os patches ou upgrades de versão menores deverão ser considerados Alterações Normais, portanto, todos os processos aplicáveis de Gerenciamento de Alterações deverão ser aplicados. Todos os softwares patches ou demais itens, que serão instalados para atender a esta necessidade, deverão ser fornecidos pela CONTRATANTE.
i) Se a CONTRATADA determinar que este item no escopo da CONTRATANTE é suscetível a uma nova vulnerabilidade, que é classificada como Baixa ou Média, deverá buscar a aprovação da CONTRATANTE antes de tomar quaisquer medidas de resposta. Caso um engenheiro do SOC considere uma nova vulnerabilidade classificada como Alta em gravidade, a CONTRATADA deverá tomar medidas de resposta imediata através de um Caso de Mudança de Emergência.

2.2.4. REQUISITOS COMUNICAÇÃO

a) Mensalmente por e-mail deverá ser entregue um relatório em português, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas.
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) A CONTRATADA deverá rever periodicamente as políticas e processos do SOC a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL 4;
e) A CONTRATADA deverá disponibilizar dashboards de acompanhamento em tempo real da operação do SOC que permitam a validação dos indicadores acordados;
f) A CONTRATADA deverá apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;
g) A CONTRATADA deverá confeccionar relatórios técnicos pontuais sob demanda;
h) A CONTRATADA deverá disponibilizar acesso de leitura a todas as ferramentas utilizadas para a prestação do serviço, permitindo desta forma que a CONTRATANTE audite a correta entrega do objeto contratado;
i) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
j) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
k) É responsabilidade da CONTRATADA supervisionar as rotinas de backup e restauração dos equipamentos, softwares e configurações implantadas referentes a segurança da informação;
l) É responsabilidade da CONTRATADA supervisionar as rotinas periódicas configuradas referentes a segurança da informação;
m) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobrea criação ou atualizações de tíquetes.
n) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
o) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da CONTRATADA.

p) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.
q) Quando o SOC cria um Relatório de Incidente de Segurança, um ticket correspondente deve ser criado no portal e uma notificação por e-mail é enviada para a CONTRATANTE.
r) O CONTRATANTE deverá comunicar um ponto focal, responsável pelo nível de serviço.

2.2.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) Os serviços devem suportar integrações com qualquer software via API.
b) Gere relatórios de vulnerabilidades encontradas minimamente em CSV:
1. Resumo executivo, com informações resumidas sobre a varredura
2. Relatório detalhado, com todas as informações técnicas necessárias para que o leitor reproduza os problemas identificados
c) O serviço deverá possuir um painel com resultados em tempo real das vulnerabilidades existentes.
d) O serviço deverá apresentar Relatório de risco incorporado na mesma plataforma.
e) O serviço deverá possuir suporte para relatórios de risco de múltiplos aplicativos.

2.2.6. REQUISITOS DE ATIVAÇÃO

a) A CONTRATADA deverá realizar a ativação e configuração de acordo com as necessidades do ambiente específico da CONTRATANTE, para assegurar que o ele esteja pronto para a implementação no ambiente.
b) A CONTRATADA deverá realizar Assistência para definir os requisitos do caso de uso da CONTRATANTE;
c) A CONTRATADA deverá realizar a Configuração dos recursos e funcionalidades dos serviços para atender ao caso de uso da CONTRATANTE.
d) A CONTRATADA deverá realizar Monitoramento de ativos baseado em dados coletados via scan ou endpoint.

2.3. SERVIÇO DE PROTEÇÃO DE PLATAFORMAS LINUX

2.3.1. REQUISITOS DE NEGÓCIO

a) O serviço deve ser compatível com diferentes distribuições Linux amplamente utilizadas, como Ubuntu, CentOS, Debian, Red Hat, entre outras.
b) Capacidade de detectar e prevenir a execução de malwares, vírus e outras ameaças conhecidas e desconhecidas nas plataformas Linux.
c) Verificação contínua da integridade dos arquivos do sistema para detectar alterações não autorizadas e atividades suspeitas.
d) Gerenciamento de contas de usuário privilegiado para evitar acessos não autorizados e garantir a segurança dos sistemas.
e) Criptografia adequada de senhas e chaves de acesso armazenadas no sistema para evitar o acesso não autorizado.
f) Atualização regular de pacotes e patches para mitigar vulnerabilidades conhecidas e minimizar a superfície de ataque.
g) Coleta e análise de logs e eventos do sistema para identificar atividades anômalas e potenciais ameaças.
h) Controle de Privilégios e Permissões:
i) Fornecimento de relatórios detalhados e painéis de controle para que os administradores possam monitorar e avaliar a eficácia do serviço.

2.3.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) Deve ser capaz de identificar e bloquear a exploração de vulnerabilidades de execução remota de código, inclusive 0-days, por meio do monitoramento e verificação das syscalls, garantindo a segurança do ambiente do órgão contra ataques sofisticados.
b) Deve operar de forma eficiente, sem causar impacto significativo no desempenho dos serviços em que for implementado.
c) Deve ser atualizada regularmente, de acordo com as últimas ameaças e vulnerabilidades conhecidas, para garantir uma proteção eficaz contra ameaças emergentes.
d) Deve permitir configurações personalizadas de acordo com as necessidades e políticas de segurança específicas de cada ambiente.
e) Deve ser compatível e integrável com os sistemas Linux existentes na infraestrutura da CONTRATANTE, evitando conflitos e garantindo a interoperabilidade adequada.

2.3.3. REQUISITOS DE SERVIÇO

a) A CONTRATADA deve fornecer especialistas qualificados em segurança Linux com experiência em proteção e monitoramento de plataformas Linux.
b) O serviço deve garantir monitoramento 24x7 das plataformas Linux para detecção proativa de ameaças e atividades suspeitas.
c) Capacidade de identificar e responder rapidamente a incidentes de segurança relacionados às plataformas Linux.
d) Realização de análises regulares de vulnerabilidades para identificar e mitigar potenciais pontos fracos nas plataformas Linux.
e) Gerenciamento adequado de atualizações e patches para garantir que as plataformas Linux estejam protegidas contra ameaças conhecidas.
f) Verificação regular da integridade dos arquivos do sistema para identificar alterações não autorizadas.
g) Coleta e análise de logs e eventos para detecção de atividades suspeitas e auxílio na investigação de incidentes.
h) Capacidade de responder a incidentes de segurança prontamente e implementar medidas de remediação adequadas.
i) Fornecimento de relatórios detalhados sobre as atividades de segurança, incluindo incidentes detectados, ações tomadas e recomendações para melhorias.
j) Integração do serviço com o Centro de Operações de Segurança (SOC) para garantir uma visão holística da postura de segurança da organização.
k) O serviço deve estar em conformidade com as regulamentações e normas de segurança relevantes aplicáveis à proteção de dados e sistemas.

2.3.4. REQUISITOS DE COMUNICAÇÃO

a) Mensalmente por e-mail deverá ser entregue um relatório em português sobre Comportamentos Anômalos encontrados, com comentários do especialista, em caso de incidentes considerados Críticos a comunicação deverá ser imediata.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas.
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) A CONTRATADA deverá rever periodicamente as políticas e processos do SOC a fim de contribuir com a

melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL 4;
e) A CONTRATADA deverá disponibilizar dashboards de acompanhamento em tempo real da operação do SOC que permitam a validação dos indicadores acordados;
f) A CONTRATADA deverá apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;
g) A CONTRATADA deverá confeccionar relatórios técnicos pontuais sob demanda;
h) A CONTRATADA deverá disponibilizar acesso de leitura a todas as ferramentas utilizadas para a prestação do serviço, permitindo desta forma que a CONTRATANTE audite a correta entrega do objeto contratado;
i) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
j) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
k) É responsabilidade da CONTRATADA supervisionar as rotinas periódicas configuradas referentes a segurança da informação;
l) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
m) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da CONTRATADA.
n) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.
o) Quando o SOC cria um Relatório de Incidente de Segurança, um ticket correspondente deve ser criado no portal e uma notificação por e-mail é enviada para a CONTRATANTE.
p) A CONTRATADA deverá comunicar um ponto focal, responsável pelo nível de serviço.

2.3.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) O serviço deve ser compatível com diversas distribuições Linux, como Ubuntu, CentOS, Debian, Red Hat, entre outras, garantindo sua aplicabilidade em diferentes ambientes.
b) Deve ser possível integrar o serviço de proteção de plataformas Linux com outras ferramentas de segurança já utilizadas pela organização.
c) O serviço deve ser capaz de proteger plataformas Linux em ambientes on-premises e em nuvem, como AWS, Azure, Google Cloud, entre outros.
d) O serviço deve permitir a configuração de políticas de segurança personalizadas para atender aos requisitos específicos da organização.
e) Deve ser compatível com soluções antimalware e antivírus já implantadas, permitindo a integração e o compartilhamento de informações sobre ameaças.
f) Deve ser integrável com plataformas de IAM para sincronização de informações de usuários e permissões de acesso.
g) Deve ser possível integrar o serviço com ferramentas de monitoramento e análise de logs para obter informações detalhadas sobre atividades de segurança.
h) O serviço deve ser integrável com sistemas de gerenciamento de configuração para garantir que as configurações de segurança estejam em conformidade com as políticas definidas.
i) Deve ser possível integrar o serviço com ferramentas de análise de vulnerabilidades para identificar e corrigir potenciais vulnerabilidades nos sistemas.
j) O serviço deve poder se integrar com sistemas de gerenciamento de TI existentes para facilitar a administração e a gestão das plataformas Linux.

k) Deve ser compatível com soluções de automação e orquestração para facilitar a implementação de políticas de segurança de forma automatizada.
l) O serviço deve ser compatível com ambientes de TI híbridos, que envolvam uma combinação de infraestrutura on-premises e em nuvem.

2.3.6. REQUISITOS DE ATIVAÇÃO

a) Verificação da compatibilidade do serviço com a distribuição Linux utilizada na plataforma alvo (por exemplo, Ubuntu, CentOS, Debian, Red Hat).
b) Ativação e configuração de todas as dependências necessárias para o funcionamento adequado do serviço.
c) Configuração adequada das interfaces de rede e endereçamento IP para permitir a comunicação entre o serviço e outros componentes da infraestrutura de segurança.
d) Configuração do firewall para permitir o tráfego de rede necessário para o funcionamento do serviço de proteção.
e) Definição das políticas de segurança adequadas para o serviço, incluindo controle de acesso, autenticação, entre outros.
f) Criação e configuração de contas de usuário e permissões necessárias para o funcionamento do serviço.
g) Configuração de alertas e notificações para informar os administradores sobre eventos de segurança importantes.
h) Habilitação de registros (logs) e auditoria para permitir a análise e o acompanhamento das atividades do serviço.
i) Realização de testes para verificar o correto funcionamento do serviço após a ativação e configuração.
j) Elaboração de documentação detalhada com os procedimentos de ativação e configuração do serviço.
k) Verificação da integração bem-sucedida do serviço com outros componentes do ambiente de segurança, como o SOC e outras soluções de proteção.
l) Verificação de que o serviço está em conformidade com as políticas e padrões de segurança da organização, incluindo testes de vulnerabilidade.

2.4. SERVIÇO DE CRIPTOGRAFIA E MASCARAMENTO DE DADOS

2.4.1. REQUISITOS DE NEGÓCIO

a) O serviço será realizado através de um Centro de Operações de Segurança (Security Operation Center - SOC) pertencente à CONTRATADA.
b) O Serviço deverá ser disponibilizado para ser usado na infraestrutura de rede da CONTRATANTE.
c) A CONTRATANTE espera que a CONTRATADA entregue o serviço, ativado e funcional.
d) Serviço para proteção dos dados e atender as demandas regulatórias e de soberania de dados.
e) Possuir um sistema de tokenização, cifragem deve ser passível de auditoria e ser desenvolvido no Brasil ou no caso de empresa estrangeira deverá disponibilizar seus códigos fontes.
f) Deve permitir a Anonimização e pseudo anonimização, gerando dados e preservando as características de verificadores de CPF e permitir gerar o padrão de CEPs do Brasil e ruas para não afetar as bases de referência.
g) Deverá controlar o acesso indevido aos recursos de dados nas premissas, em nuvem pública ou privada, por exemplo no AWS e AZURE, e deve guardar as suas chaves criptográficas, de forma adequada, ter-se o domínio e total controle destas chaves.
h) Deve permitir a criptografia de dados em bases de dados estruturadas, via chamadas à API, UDF, ETL proprietário, Drivers ou ferramentas externas.
i) Deve conter sistema de cifragem de arquivos não estruturados, via software de criptografia ou sistema de arquivos, para Windows e Linux.

j) Deve permitir localizar e inventariar certificados digitais em servidores de aplicação HTTPs e no repositório do Windows, para adequada manutenção de seu vencimento.

2.4.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) Deve permitir criar políticas de automação programadas para rotacionar chaves de criptografia, e emissão de certificados digitais em AC interna ou externa.

b) O serviço deve conter um Gestor de chaves em KMS, compatível HSM em hardware em nuvem, para armazenamento de chaves, onde os equipamentos adotados na prestação dos serviços deverão estar no território brasileiro, e ser certificados pelo INMETRO em acordo com a regulação brasileira e o ITI/ICPBRASIL.

c) Deve ter interface WEB.

d) Deve permitir separar as chaves em grupos e sessões.

e) Deve ter interface tipo relatório (report), para visualização das chaves ou certificados que vão expirar num intervalo de tempo.

f) O Gestor de chaves deve ser capaz de integrar com HSMs externos, com no mínimo 3 fabricantes diferentes.

g) O Gestor de chaves deve gerar automaticamente de certificados digitais, SSL com distribuição automatizada em servidores remotos, e atualização de serviços como ISS, sem interação humana.

h) Deve atender ao KMIP 1.4

i) Deve suportar ABAC e RBAC

j) Deve ser uma solução virtual com opção de hardware específico para atendimento de necessidade do serviço.

k) Deve suportar CEF para integração com SIEM

l) Deve suportar até 50 milhões de chaves

m) Deve suportar REST Api para a gestão das chaves, criação e atributos

n) Deve integrar com LDAP, e ter MFA para autenticar usuários

o) Deve fazer gestão de chaves de forma nativa via KMIP de BASES DE DADOS, IBMDB2, Mongo, MySQL e ou agentes para SQL e Oracle.

p) O serviço deve ser híbrido que atenda sistemas em nuvem e on-site de gestão de chaves criptográficas, fazendo todo controle de forma nativa, para vários fabricantes, como por exemplo VMware, Nutanix, DELL.

q) O serviço deve gerenciar e automatizar toda a gestão de criptografia, certificados digitais e chaves simétricas.

r) Deve permitir gerenciar chaves de VPN, chaves de SSH, base de dados, certificados digitais, SSL e storage NAS, Vsan.

s) Deve permitir e controlar acesso aos servidores que usam SSH.

t) Deve Permitir execução de scripts Java dedicados, internamente no KMS, editáveis e configuráveis, evitando erros que podem prejudicar a proteção dos dados, para procedimentos de automação.

u) Tokenização de dados.

v) Deve ter agente de criptografia de dados (Format Preserve Encryption), FF1 e não pode ser usado o padrão FF3 para cifragem de dados.

w) Deve possuir API EKM para MS-SQL.

x) Deve suportar login do usuário com perfil de operação no dado, no mínimo para cifrar e decifrar.

y) Deve suportar a criptografia com preservação do formato reversível e irreversível.

z) Deve suportar autenticação baseada em DNA do servidor, com associação ao usuário, evitando o login não autorizado de servidores e usuários.

aa) Deve suportar autenticação PKI, LDAP e Kerberos.

bb) Deve permitir pela console do AD criar grupos no LDAP com perfil dedicado da operação na chave, permitindo que um usuário do AD seja capaz decifrar com uma determinada chave ou não.

cc) Deve suportar SysLog.

dd) Deve possuir agente ETL (Extract Transform and Load) para base (MySQL, CSV, IBMDB2,POSTGRE, SQL

e Oracle) de criptografia com preservação de formato.
ee) Deve permitir Driver MySQL, MSSQL(JAVA), ODBC e JDBC customizados para acesso às bases.
ff) Deve permitir cifrar arquivos usando o AES-256 NI
gg) Deve utilizar o FF1
hh) Deve gerar CPFs com dígitos válidos
ii) Dever gerar CEPs válidos
jj) Deve suportar strings de até 4000 caracteres
kk) Deve suportar o alfabeto português e caracteres usados em nomes no Brasil
ll) Deve permitir cifrar parcialmente um dado, através de um parâmetro de máscara
mm) Deve permitir mascaramento de dados
nn) Deve permitir cifrar e-mails reservando sua formatação
oo) Deve possuir API nativa Linux e Windows
pp) Deve possuir Webservice com autorização usando Bearer token
qq) Descoberta de certificados digitais
rr) Deve identificar a data de validade e assuntos de um certificado padrão X509 e alertar usuários sobre sua expiração;
ss) Deve enviar alertas via e-mail;
tt) Deve ser capaz de enviar e-mails de alerta para no mínimo 2 níveis de alerta, um primeiro de menor severidade e um segundo de maior severidade quando o tempo para expiração for menor que a metade do prazo ajustado do alerta;
uu) Deve enviar alertas de prazo de expiração com antecedência ajustável;
vv) Deve ser capaz de enviar e-mail via SMTP, com contas com e sem autenticação;
ww) Deve Enviar mensagens com o log de ERRO e a lista Servidores não encontrados;
xx) Deve enviar mensagens com lista de todos os servidores Analisados;
yy) Deve permitir configurar Mensagem enviada no corpo do e-mail e nome do remetente;
zz) Deve possuir Dashboard de administração das configurações e visualização do inventário de certificados;
aaa) Deve permitir visualizar a quantidade de certificados analisados, separados por expirados, a expirar e em eminência de expirar, servidores analisados e falhas;
bbb) Funcionar em no mínimo em MS IIS;
ccc) Deve gerar backup das configurações;
ddd) O Dashboard deve integrar e herdar as regras do perfil do Active Directory (AD) para definições de acessos, administrador ou usuário;
eee) Para atendimento de necessidade de serviço prestado, pode ser instalado em servidor local ou em ambiente cloud (nuvem);
fff) Permitir a gestão remota dos Agentes;
ggg) Fazer varredura, em determinada rede para localizar certificados em pastas, servidores SSL e no repositório de chaves do Windows;
hhh) Deve listar certificados do repositório do Windows, no contexto da máquina e do usuário logado e não logado;
iii) Deve fazer varredura por rede, por range de IP e de forma local;
jjj) Deve permitir a criação de listas de redes para varredura;
kkk) Deve permitir a exclusão de IPs da varredura em lista separada; lll) Deve gerar log da varredura;
mmm) Deve permitir agendar a varredura, por dia e hora em escala semanal ou por intervalo de tempo;
nnn) Deve gerar listas em CSV com informações do certificado, com a data de expiração, sujeito, tumbprint, username, conta usuário do sistema operacional e local onde foi encontrado;

ooo) Deve criar lista individual para certificados expirados e a expirar;
ppp) Deve criar lista de computadores, IPs, não localizados;
qqq) Permitir armazenar localmente ou remotamente as listas do inventário de certificados;
rrr) Permitir a customização dos itens de varredura com perfis pré-determinados a partir de estações distintas;
sss) Exclusão de máquinas e/ou customização unitária de varredura;
ttt) Identificar certificados da cadeia ICP_Brasil;
uuu) Permitir a varredura de certificados em ambientes Linux e no Windows, MS-KeyStore.

2.4.3. REQUISITOS DE SERVIÇO

a) O serviço de criptografia e mascaramento de dados deve estar disponível e operacional 24 horas por dia, 7 dias por semana, sem interrupções.
b) A CONTRATADA, na execução dos serviços a serem prestados, deve fornecer tecnologias de criptografia robustas para proteger dados sensíveis em repouso, em trânsito e em uso.
c) Deve haver recursos de mascaramento de dados para ocultar informações confidenciais em ambientes de teste, desenvolvimento ou compartilhamento de dados.
d) A gestão de chaves de criptografia deve ser realizada de forma segura, com a capacidade de gerar, armazenar e revogar chaves conforme as necessidades da CONTRATANTE.
e) O SOC da CONTRATADA deve realizar monitoramento contínuo das atividades de criptografia e mascaramento para identificar comportamentos anômalos ou falhas de segurança.
f) O serviço deve incluir recursos para detectar tentativas de ataque à criptografia e alertar prontamente a CONTRATANTE sobre eventuais ameaças.
g) O serviço deve garantir a capacidade de auditar e rastrear o uso da criptografia e mascaramento de dados para fins de conformidade e investigação de incidentes.
h) O serviço deve ser compatível e integrável com os diversos ambientes e sistemas da CONTRATANTE, garantindo a proteção dos dados em toda a infraestrutura.
i) As chaves de acesso para criptografia devem ser armazenadas de forma segura, com medidas adequadas para protegê-las contra acesso não autorizado.
j) Deve ser estabelecido um conjunto claro de políticas para o uso adequado da criptografia e mascaramento de dados, incluindo acesso autorizado e privilégios de uso.
k) O SOC deve ter capacidade de resposta rápida a incidentes relacionados à criptografia e mascaramento, tomando ações adequadas para mitigar danos e restaurar a segurança.
l) O serviço deve realizar testes regulares de segurança e vulnerabilidade para garantir a robustez e eficácia das medidas de criptografia e mascaramento.
m) O serviço deve fornecer relatórios periódicos sobre o desempenho do serviço, métricas de segurança e eficácia das medidas implementadas.
n) O serviço deve permitir a definição de controles de acessos granulares para garantir que apenas pessoas autorizadas tenham acesso a dados criptografados.
o) O serviço deve estar em conformidade com os padrões de segurança relevantes, como PCI DSS, HIPAA, GDPR, entre outros, dependendo das necessidades da CONTRATANTE.
p) Deve ser garantida a realização de backups regulares das chaves de criptografia, bem como a capacidade de recuperá-las em caso de perda ou corrupção.

2.4.4. REQUISITOS DE COMUNICAÇÃO

a) Sempre que solicitado pela CONTRATANTE a CONTRATADA, por e-mail ou outro meio estabelecido previamente, deverá ser entregue um relatório em português sobre status do serviço, com métricas e sugestões de

melhoria, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas;
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) A CONTRATADA deverá rever periodicamente as políticas e processos do SOC a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL 4;
e) A CONTRATADA deverá disponibilizar dashboards de acompanhamento em tempo real da operação do SOC que permitam a validação dos indicadores acordados;
f) A CONTRATADA deverá apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;
g) O servico deverá prever a confecção de relatórios técnicos pontuais sob demanda;
h) A CONTRATADA deverá disponibilizar acesso de leitura a todas as ferramentas utilizadas para a prestação do serviço, permitindo desta forma que a CONTRATANTE audite a correta entrega do objeto contratado;
i) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
j) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
k) É responsabilidade da CONTRATADA supervisionar as rotinas de backup e restauração dos equipamentos, softwares e configurações implantadas referentes a segurança da informação;
l) É responsabilidade da CONTRATADA supervisionar as rotinas periódicas configuradas referentes a segurança da informação;
m) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobre a criação ou atualizações de tiquetes.
n) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
o) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da contratada.
p) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.
q) Quando o SOC cria um Relatório de Incidente de Segurança, um ticket correspondente deve ser criado no portal e uma notificação por e-mail é enviada para a CONTRATANTE.
r) O CONTRATANTE deverá comunicar um ponto focal, responsável pelo nível de serviço.

2.4.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) O serviço deve ser compatível e integrável com os diversos ambientes de TI da CONTRATANTE, incluindo sistemas operacionais, servidores, bancos de dados e aplicativos.
b) Deve ser possível utilizar o serviço em ambientes de nuvem pública, privada ou híbrida, garantindo a proteção de dados independentemente da infraestrutura utilizada.
c) O serviço deve fornecer APIs e web services bem documentados para facilitar a integração com os sistemas e aplicações existentes na infraestrutura da CONTRATANTE.
d) Deve ser possível integrar o serviço com diferentes tipos de bancos de dados, como Oracle, SQL Server, MySQL, PostgreSQL, entre outros.
e) O serviço deve ser capaz de criptografar e mascarar dados em sistemas de arquivos locais, compartilhados e

em servidores de rede.
f) Deve haver compatibilidade com plataformas de e-mail e mensageria utilizadas pela CONTRATANTE, garantindo a segurança de comunicações sensíveis.
g) O serviço deve integrar-se com sistemas de IAM para gerenciar com eficiência as chaves de criptografia e o acesso aos dados mascarados.
h) O serviço deve ser compativel com padrões e normas de segurança amplamente reconhecidos, como FIPS 140-2, AES, SHA, entre outros.
i) Deve ser possível integrar o serviço de criptografia e mascaramento em aplicativos móveis para proteger dados sensíveis em dispositivos móveis.
j) O serviço deve ser capaz de integrar-se com sistemas de monitoramento e SIEM (Security Information and Event Management) para fornecer informações detalhadas sobre as atividades de criptografia e mascaramento.
k) Deve ser possível integrar o serviço a ferramentas de auditoria e compliance para monitorar e garantir a conformidade com políticas de segurança e regulamentações.
l) O serviço deve ser compatível com diferentes protocolos de rede, como TCP/IP, UDP, HTTP(S), FTP, para garantir a proteção de dados em trânsito.
m) Caso haja a necessidade de utilização de hardware específico para acelerar a criptografia, o serviço deve ser compatível com essa infraestrutura.

2.4.6. REQUISITOS DE ATIVAÇÃO

a) A CONTRATADA deve realizar uma avaliação prévia dos ambientes de TI da CONTRATANTE para identificar os requisitos específicos de ativação.
b) Devem ser definidos e comunicados à CONTRATANTE os requisitos mínimos de hardware, software e rede para ativação e operação do serviço.
c) Deve ser elaborado um plano detalhado de ativação, incluindo cronograma, atividades, responsabilidades e recursos necessários.
d) A CONTRATADA deve definir se a ativação do serviço será realizada remotamente ou se será necessária a presença de técnicos no local.
e) A configuração inicial do serviço de criptografia e mascaramento deve ser realizada de acordo com as necessidades e políticas de segurança da CONTRATANTE.
f) Deve ser conduzido um conjunto abrangente de testes após a ativação para verificar a correta implementação do serviço e a integração com os sistemas da CONTRATANTE.
g) O serviço deve ser integrado de forma adequada com os sistemas e aplicações existentes na infraestrutura da CONTRATANTE, garantindo a sua compatibilidade.
h) Deve ser implementado um procedimento de backup e recuperação do serviço, a fim de garantir a disponibilidade dos dados mesmo em caso de falhas.
i) Todo o processo de ativação, configuração e integração deve ser devidamente documentado para facilitar futuras referências e manutenções.
j) Antes de colocar o serviço em produção, devem ser realizados testes de segurança e vulnerabilidade para garantir a sua robustez e segurança.
k) A ativação do serviço deve passar por um processo de homologação final pela CONTRATANTE para verificar se atende aos requisitos e expectativas.
l) Após a ativação, o SOC da CONTRATADA deve realizar um monitoramento contínuo do serviço para identificar possíveis problemas e garantir a sua eficiência.
m) Deve ser estabelecido um procedimento para aplicação de atualizações e patches do serviço, garantindo que esteja sempre atualizado e protegido contra vulnerabilidades conhecidas.

n) A CONTRATADA deve fornecer suporte pós-ativação, com atendimento ágil e eficiente para resolver quaisquer problemas que possam surgir.

2.5. SERVIÇO DE TESTE DE INSTRUÇÃO

2.5.1. REQUISITOS DE NEGÓCIO

a) A CONTRATADA e a CONTRATANTE devem concordar com o escopo e os detalhes dos testes unitários a serem realizados, especificando os sistemas, aplicações e redes envolvidos na prestação do serviço.

b) O serviço deve ser contratado com base na realização de testes unitários individuais, permitindo à CONTRATANTE selecionar os testes específicos a serem realizados, de acordo com suas necessidades.

c) As técnicas de teste a serem aplicadas em cada teste unitário devem ser detalhadas e acordadas previamente entre as partes.

d) O serviço deve permitir que a CONTRATANTE agende a realização de cada teste unitário de acordo com sua disponibilidade e prioridades.

e) Para cada teste unitário realizado, a CONTRATADA deve fornecer relatórios detalhados, incluindo as vulnerabilidades encontradas, impactos e recomendações de correção.

f) A CONTRATADA deve atualizar regularmente a CONTRATANTE sobre o progresso dos testes unitários contratados e qualquer problema que possa surgir.

g) A CONTRATADA deve garantir a confidencialidade e sigilo das informações relativas aos testes unitários realizados, protegendo os dados sensíveis da CONTRATANTE.

h) Antes de iniciar cada teste unitário, a CONTRATANTE deve revisar e aprovar o plano e a abordagem propostos pela CONTRATADA.

i) Os resultados dos testes unitários devem ser integrados aos relatórios de segurança da CONTRATANTE, permitindo uma visão completa das vulnerabilidades e riscos.

j) A CONTRATADA deve fornecer suporte e orientação à CONTRATANTE, esclarecendo dúvidas e oferecendo assistência técnica relacionada aos testes unitários.

k) A CONTRATANTE deve ter a opção de contratar testes unitários adicionais à medida que novos serviços sejam desenvolvidos ou adquiridos.

l) A CONTRATADA deve cumprir os prazos acordados para a realização de cada teste unitário, garantindo a eficiência do serviço.

m) Garantir que o serviço de teste de intrusão esteja sempre atualizado e em conformidade com as melhores práticas de segurança cibernética, incluindo a incorporação de novas técnicas e ferramentas.

2.5.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) Realização de teste de penetração digital semi-orientado “Grey-box penetration test” com equipe de ataques ofensivos “red team” realizando testes manuais e ferramentas automatizadas no site e na infraestrutura que o suporta (sistemas operacionais, servidores web, servidores de aplicação, servidores de banco de dados, entre outros), para elaboração de relatórios e posterior direcionamento da correção das fragilidades detectadas;

b) Realização de teste de penetração digital cego “Black-box penetration test” com equipe de ataques ofensivos “red team” realizando testes manuais e ferramentas automatizadas no site e na infraestrutura que o suporta (sistemas operacionais, servidores web, servidores de aplicação, servidores de banco de dados, entre outros), para elaboração de relatórios e posterior correção das fragilidades detectadas;

c) Testes de Invasão Externos e Internos e tem como objetivo principal identificar, possíveis vulnerabilidades na infraestrutura tecnológica da CONTRATANTE e seus clientes.

d) O Teste de Negação de Serviço (DoS) deve compreender a verificação da quantidade e do tipo de tráfego suportado pela infraestrutura do CONTRATANTE, apresentar os riscos e as soluções para minimizar o impacto de um ataque de indisponibilidade real.

e) Teste de Penetração Interno.
f) O serviço deverá prever a realização de ao menos 1 teste intrusão a cada 6 meses para identificação de vulnerabilidades por meio de simulações de invasão de aplicações e infraestrutura (Teste de Invasão) a serem executadas internamente (através da rede interna da CONTRATANTE).
g) Condução de GAP Analysis de segurança e frameworks específicos.
h) Consultoria para apoio de GAP analysis para frameworks específicos conforme a necessidade.
i) Análise riscos de segurança.
j) Realização de Risk Analysis associado a vulnerabilidades encontradas em ambientes de IT (Análise de Vulnerabilidades Tecnológicas) e com os resultados da Análise de Conformidade.
k) A metodologia e framework utilizado para o serviço de Análise de Riscos em Segurança deve ser a ISO/IEC 27005.
l) Sua abordagem e metodologia devem ser usadas em combinação com outros padrões de segurança de TI, como a série ISO 27000 que tem o foco em:
1. Confidencialidade (C), Integridade (I), Disponibilidade (D)
2. Sistema de gerenciamento de segurança da informação (SGSI)
3. Classificação de informações, análise de riscos, conceito de segurança
4. Abordagem Plan-Do-Check-Act para segurança de TI
m) A CONTRATADA deverá realizar de forma recorrente automatizada e manual a identificação de vulnerabilidades por meio de simulações de invasão de aplicações e infraestrutura, as ações manuais deverão ter testes diários pela equipe contratada a fim de mitigar ao máximo as principais aplicações se sistemas críticos.
n) A CONTRATADA deverá, em caso de impossibilidade por parte da CONTRATANTE de aplicação das mitigações sugeridas, sugerir medidas alternativas de mitigação de risco.
o) A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contramedidas ou deficiências na infraestrutura ou sistemas da CONTRATANTE;
p) O serviço deverá minimamente tentar a evasão de regras do firewall, acesso a roteadores, sistemas operacionais e demais serviços de redes, captura de senhas etc.
q) O serviço deverá realizar ataques de man in the middle (ARP Spoofing, captura de informações trafegando na rede) e tentativas de burlarfirewall para a saída de informações.
r) O serviço deverá realizar dois tipos de teste de intrusão: tentativa de intrusão/penetração através do ambiente interno e tentativa de intrusão através do ambiente externo;
s) O serviço deverá realizar os testes de intrusão/penetração externos, baseando- se nos endereços (URL's) e ranges de IP's públicos da CONTRATANTE registrados no registro.br e NIC.br.
t) O serviço realizar os testes de intrusão/penetração externos, de forma a explorar possíveis vulnerabilidades nos serviços disponíveis.
u) O serviço deverá testar servidores, estações e outros equipamentos da estrutura da rede conforme aprovação e indicação da CONTRATANTE, com o objetivo de obter acesso a informações controladas de acordo com quantitativos informados.
v) O serviço deverá testar ativos de rede das unidades da CONTRATANTE, como por exemplo estações de trabalho, roteadores e switches gerenciáveis, de acordo com amostragem de referência informada pela CONTRATANTE.
w) Os alvos dos "Testes de Invasão", bem como as premissas e condições para realização dos mesmos serão definidas e aprovadas pelo CONTRATANTE. Todas as fases dos "Testes de Invasão" poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo, deverá a CONTRATADA ser reportada pelo CONTRATANTE,

haja vista a necessidade de manter a disponibilidade dos ambientes, ativos e serviços do ambiente operacionais.
x) Os Testes deverão ser realizados, minimamente, por meio das seguintes abordagens:
1. Tentativa de intrusão na camada da rede e tentativa de intrusão na camada do aplicativo;
y) Os Testes de Intrusão poderão ser direcionados aos servidores Web e respectivas aplicações do serviço de hospedagem contratado pela CONTRATANTE.

2.5.3. REQUISITOS DE SERVIÇO

a) Deverão ser testados, minimamente, os seguintes quesitos, quando pertinentes:
1. Validação de acesso lógico
2. Segmentos de rede
3. VLANs
4. Burlar regras de firewall
5. Obtenção de informações
6. Enumeração de usuários
7. Sniffing
8. ARP Spoofing
9. Segurança dos dados
10. Canal de comunicação
11. Cifras fracas
12. Armazenamento inseguro
13. Descoberta de Senhas
14. Força bruta
15. Ataque off-line
16. Arquitetura da rede
17. Acesso remoto e VPN
18. Protocolos de comunicação
19. Mixed Content/Scripting;
20. Unvalidated Redirects;
21. Insecure Cookies;
22. Iframe Injection;
23. Clickjacking;
24. Cross Site Scripting (XSS);
25. Cross Site Request Forgery (XSRF);
26. Cross Site Script Inclusion (XSSI);
27. HTTP Parameter Pollution;
28. Path Traversal;
29. Buffer Overflow;
30. Integer Overflow;
31. Privilege Escalation;
32. Authentication Bypass;
33. Information Leak;
34. Local File Inclusion;
35. Remote File Inclusion;
36. Source Code Disclosure;
37. SQL Injection;

38. Remote Code Execution;
39. Vulnerabilidades de lógica difusa;
40. Vulnerabilidades de regra de negócio;
41. Revisão das vulnerabilidades listadas no OWASP Top 10
42. Insecure Direct Object Reference.

b) O escopo do serviço e seus objetivos devem ser definidos com clareza, detalhando quais sistemas e redes serão testados e quais tipos de ataques serão simulados.

c) Deve ser obtida autorização prévia por escrito dos proprietários dos sistemas e redes a serem testados para garantir que o serviço seja conduzido legalmente.

d) O serviço a ser realizado no teste de intrusão deve contemplar profissionais experientes, certificados e qualificados para realizar esse tipo de serviço.

e) O serviço deve ser conduzido seguindo metodologias reconhecidas pela indústria de segurança, como a metodologia PTES (Penetration Testing Execution Standard) ou outras similares.

f) Antes de iniciar o teste de intrusão, uma análise de riscos deve ser realizada para identificar os possíveis impactos e consequências dos ataques simulados.

g) Os testes de intrusão devem simular ataques reais que hackers poderiam utilizar, para avaliar a resiliência dos sistemas e a capacidade de detecção e resposta.

h) Os testes de intrusão devem ser conduzidos de forma a não interferir nas operações regulares da organização, evitando qualquer prejuízo ao ambiente em produção.

i) Após a conclusão dos testes, devem ser entregues relatórios detalhados com os resultados, descrevendo as vulnerabilidades encontradas, as técnicas utilizadas e as recomendações de correção.

j) Todas as vulnerabilidades encontradas durante os testes devem ser identificadas e documentadas de forma clara e precisa.

k) O serviço deve fornecer recomendações detalhadas de como mitigar as vulnerabilidades encontradas, permitindo que a organização tome as medidas necessárias para corrigir os problemas.

l) O serviço de teste de intrusão deve ser conduzido de forma sigilosa e confidencial, garantindo que as informações sensíveis da organização sejam protegidas.

m) O serviço deve avaliar a segurança em diferentes camadas da infraestrutura, incluindo testes de rede, aplicativos web, dispositivos móveis e outros sistemas relevantes.

n) Os testes de intrusão devem estar em conformidade com as regulamentações e leis aplicáveis, evitando qualquer atividade que possa ser considerada ilegal.

o) Quando aplicável, o serviço deve incluir testes de engenharia social para avaliar a segurança em relação a manipulação de funcionários ou usuários.

p) Deve haver acompanhamento pós-teste para garantir que as vulnerabilidades identificadas tenham sido corrigidas e que a segurança tenha sido aprimorada.

q) É importante realizar testes de intrusão periodicamente, especialmente após atualizações significativas na infraestrutura ou em sistemas críticos.

2.5.4. REQUISITOS DE COMUNICAÇÃO

a) A CONTRATADA deverá elaborar um relatório de auditoria com os testes realizados, vulnerabilidades encontradas e recomendações de melhoria. O relatório técnico deve ser detalhado e deve ser acompanhado de uma apresentação executiva sobre os testes executados e seus resultados, assim como recomendações de medidas de correção e deve possibilitar à CONTRATANTE conhecer suas fragilidades e permitir criar os controles de segurança necessários para minimizar o risco de invasão.

b) Todas as vulnerabilidades encontradas no pentest manual deverão ser entregues em um relatório com medidas

de correções assim como o exploit utilizado ou prova de conceito para reproduzir a falha.
c) A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo:
1. Objetivos,
2. Premissas e escopo do teste;
3. Metodologia de análise de vulnerabilidades;
4. Descrição das ações realizadas;
5. Vulnerabilidades encontradas;
6. Categorização e severidade das vulnerabilidades,
7. Recomendações e controles de segurança necessários para correção das vulnerabilidades;
8. Apresentação das evidências apuradas;
9. Fontes de pesquisa,
10. Referências e ferramentas utilizadas.
d) A CONTRATADA deverá elaborar o "Plano de Teste de Invasão", para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como:
1. Objetivos, premissas e escopo do teste;
2. Metodologia de análise de vulnerabilidades;
3. Equipe envolvida;
4. Prazos do teste.
e) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas.

2.5.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) O serviço deve ser compatível com diferentes plataformas e sistemas operacionais utilizados pela organização, como Windows, Linux, macOS, etc.
b) Deve ser possível realizar testes de intrusão em diversos tipos de infraestruturas de rede, incluindo redes locais, redes sem fio (Wi-Fi) e redes em nuvem.
c) O serviço deve ser capaz de realizar testes de intrusão em aplicações web, avaliando sua segurança contra vulnerabilidades como injeção de SQL, cross-site scripting (XSS), entre outras.
d) Deve ser possível realizar testes de intrusão em aplicativos móveis, tanto para Android quanto para iOS, para verificar a segurança em dispositivos móveis.
e) O serviço deve ser compatível com diferentes sistemas de banco de dados, como MySQL, Oracle, SQL Server, entre outros, para avaliar sua segurança contra ataques.
f) Deve ser possível testar a segurança de dispositivos de rede, como roteadores, switches, firewalls e outros dispositivos de rede.
g) Os testes de intrusão devem ser realizados em conformidade com os padrões de segurança relevantes, como a metodologia PTES (Penetration Testing Execution Standard) ou outras normas aplicáveis.
h) O serviço deve ser capaz de automatizar parte dos testes de intrusão e ser escalável para lidar com uma grande quantidade de sistemas e redes.
i) Deve ser possível gerar relatórios detalhados a partir dos resultados dos testes e integrá-los à documentação de segurança da organização.
j) O serviço deve permitir a revisão e o acompanhamento periódico dos resultados dos testes de intrusão para garantir que as vulnerabilidades sejam corrigidas adequadamente.
k) A CONTRATADA deve fornecer atualizações regulares para o serviço de teste de intrusão, garantindo que ele esteja sempre atualizado em relação às últimas ameaças e vulnerabilidades.

2.5.6. REQUISITOS DE ATIVAÇÃO

a) A rede de teste deve ser configurada adequadamente para permitir a realização dos testes de intrusão, incluindo definição de sub-redes e configuração de firewalls.
b) Deve-se garantir que todas as ferramentas e softwares utilizados no serviço estejam devidamente licenciados e atualizados para evitar problemas de conformidade.
c) Acesso ao ambiente de teste deve ser restrito a membros autorizados da equipe de teste de intrusão para garantir a segurança das informações.
d) Devem ser estabelecidas políticas e procedimentos para o uso seguro do ambiente de teste, incluindo a definição de limites de testes e ações a serem evitadas.
e) Deve ser implementado um sistema de monitoramento para acompanhar os testes em tempo real e registrar as atividades realizadas durante o serviço.

2.6. SERVIÇO DE GESTÃO DE SENHAS

2.6.1. REQUISITOS DE NEGÓCIO

a) O serviço deve ser escalável para atender às demandas de gerenciamento de senhas de um grande número de usuários, conforme a CONTRATANTE necessite.
b) A CONTRATANTE deve ter a opção de contratar o serviço em lotes de usuários, permitindo um gerenciamento mais flexível e adaptado ao crescimento da organização.
c) O serviço deve ser capaz de se integrar com o Active Directory ou outras fontes de autenticação utilizadas pela CONTRATANTE para garantir um gerenciamento centralizado.
d) A CONTRATANTE deve poder personalizar as políticas de senhas, como complexidade, expiração e histórico, de acordo com suas diretrizes de segurança.
e) O serviço deve fornecer um mecanismo para a gestão de reset de senhas, permitindo que os usuários recuperem suas senhas de forma segura e eficiente.
f) Deve ser possível implementar autenticação multifator (MFA) para aumentar a segurança no acesso às contas dos usuários.
g) O serviço deve registrar todas as atividades relacionadas ao gerenciamento de senhas, permitindo uma auditoria adequada para fins de segurança e conformidade.
h) As senhas e informações relacionadas devem ser armazenadas e transmitidas de forma criptografada, garantindo a proteção dos dados sensíveis.
i) A CONTRATANTE deve ter acesso a suporte técnico para solucionar dúvidas, problemas ou para obter assistência relacionada ao serviço de gestão de senhas.
j) O serviço deve ser integrável com sistemas, aplicativos e serviços utilizados pela CONTRATANTE para facilitar o acesso seguro.
k) O serviço deve estar em conformidade com os padrões de segurança relevantes, como ISO 27001, PCI DSS ou outras normas aplicáveis.
l) A CONTRATANTE deve ter acesso a relatórios e painéis de controle que mostrem o status e a segurança das senhas gerenciadas.
m) O serviço deve ter procedimentos para a resolução de incidentes de segurança relacionados ao gerenciamento de senhas.
n) A CONTRATANTE deve garantir a privacidade dos dados dos usuários e obter o consentimento apropriado para gerenciar suas senhas.

2.6.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) Gestão de Credenciais: O serviço deve suportar a gestão e troca de senhas dos seguintes tipos de contas:

1. Active Directory (todas as contas)
2. Contas de Usuários e Administradores Windows Locais (2008 R2+)
3. Contas de Usuários e Administradores Linux Locais (Qualquer Distribuição)
4. Contas de Usuários e Administradores Uinux Locais (QualquerDistribuição)
5. Contas de Dispositivos de Redes (Cisco, Juniper, Blue Coat, Enterasys,etc.)
6. Contas de Hypervisor (Hyper-V, VMware, Xen, etc.)
7. Contas de Sistemas de gestão off-line (iDrac, HP iLO, etc.)
8. Chaves de acesso AWS IAM
9. Contas de MS Azure AD/Office 365
10. Contas de Salesforce
11. Contas de Bancos de Dados (ODBC, MySQL, MS SQL, IBM, SAP, Oracle, PostgreSQL, etc.)
12. Contas VMWare ESX/ESXi
13. Contas LDAP (OpenLDAP, Oracle Directory Server EE, etc.)
14. Contas Mainframe (z/OS RACF)
15. O serviço proposto deve prover um framework de scripts que permite extender as funcionalidades de gestão de credenciais a outras aplicações sem a necessidade de contratação de serviços profissionais.

b) Controle de Acessos: O serviço deve ter integração nativa com Active Directory e suportar LDAP(S).

c) Deve integrar com os Grupode Segurança do Active Director como componente do controle de acessos baseado em funções (roles)

d) A integração do Active Directory do serviço proposto deve permitir uma programação de sincronização configurável para automatizar a integração de novos usuários.

e) O serviço proposto deve suportar autenticação integrada do Windows para acesso à plataforma.

f) O serviço proposto deve suportar autenticação local e grupos de controle de acesso baseados em funções (roles) locais.

g) O serviço proposto deve suportar qualquer Provedor de Identidade SAML 2.0 para Single Sign-on.

h) O serviço proposto deve oferecer suporte a qualquer solução de autenticação multifator baseada em RADIUS.

i) O serviço proposto deve suportar integrações prontas para uso com DUO, FIDO2, RADIUS e qualquer solução TOTP.

j) O serviço proposto deve oferecer suporte à lista de permissões de endereço IP para usuários de acesso.

k) O serviço proposto deve suportar o mascaramento de domínios de login disponíveis durante o processo de login do usuário.

l) O serviço proposto deve suportar um banner informativo personalizado na tela de login sem modificações de CSS.

m) O serviço proposto deve ser configurável para impor HTTPS por meio de HSTS.

n) Gestão de Políticas e Fluxos de Aprovação: O serviço proposto deve oferecer suporte a um único painel para configuração de políticas em toda a implantação.

o) A configuração da política do serviço proposto deve incluir a capacidade de definir configurações de gerenciamento de senha, configurações de segurança e localização para atribuição de carga de trabalho.

p) O serviço proposto deve oferecer suporte à aplicação de políticas em nível de conta e/ou nível de pasta.

q) O serviço proposto deve suportar os seguintes fluxos de trabalho de segurança:

1. Justificativa de acesso (o usuário deve enviar um motivo/comentário antes de acessar)
2. Aprovação de acesso -- aprovação única
3. Aprovação de acesso -- aprovação em várias etapas. Descreva como esse fluxo de trabalho é configurado em

sua plataforma.
4. Check-out e check-in de conta (senha única e exclusividade)
5. Check-out de conta com a capacidade de executar scripts carregados (PowerShell, SSH, SQL) durante o processo de pré e pós check-out.
r) O check-out do serviço proposto deve suportar um processo de check-in manual, forçado e automático baseado em tempo.
s) Os fluxos de trabalho de justificação e aprovação de soluções propostas devem oferecer suporte à validação opcional de casos/tíquetes com um sistema de emissão de tíquetes externo durante o processo de justificação e aprovação.
t) O serviço proposto deve oferecer suporte a integrações de sistemas de tickets personalizados.
u) O serviço proposto deve fornecer fluxo de trabalho e gerenciamento de políticas para solicitação, provisionamento e descomissionamento de contas de serviço descobertas e recém-criadas.
v) Auditoria e Relatórios: o serviço proposto deve incluir uma auditoria robusta e inviolável de todas as atividades dentro e contra a plataforma.
w) A auditoria do serviço proposto deve fornecer quem, o quê, onde e quando da atividade.
x) O serviço proposto deve suportar o encaminhamento de logs para qualquer plataforma SIEM.
y) O serviço proposto deve suportar captura de pressionamento de tecla para sistemas operacionais Linux, Unix e Windows.
z) O serviço proposto deve suportar a busca cruzada de teclas digitadas e permitir a exportação para um arquivo CSV.
aa) O serviço proposto deve oferecer suporte à revisão da trilha de auditoria em um único painel.
bb) O serviço proposto deve incluir um componente de Análise de Comportamento baseado em SaaS ou solução associada.
cc) O serviço de análise de comportamento deve fornecer um rico conjunto de painéis informativos, incluindo principais usuários, principais contas, mapeamento de endereço IP, alertas, etc.
dd) O serviço de análise de comportamento deve fornecer uma lista de observação para usuários recém-integrados e usuários existentes cuja atividade pode ser suspeita.
ee) O serviço de análise de comportamento deve fornecer uma trilha de auditoria indefinida da atividade dentro da plataforma.
ff) O serviço de análise de comportamento deve fornecer uma interface gráfica de acesso para visualizar comunidades de usuários que acessam contas semelhantes.
gg) O serviço de análise de comportamento deve fornecer uma interface de mapa de IP de acesso para visualizar comportamento anômalo em uma GUIde sobreposição de mapa mundial.
hh) O serviço de análise de comportamento deve fornecer uma visão geral dos usuários com contas móveis em cache ativas.
ii) O serviço de análise de comportamento deve fornecer um processo de remediação automatizado contra atividades anômalas na solução PAM suportando:
1. Notificação de Email
2. Solicitando MFA
3. Bloqueio de conta
4. Sessão de gravação
5. Forçando a aprovação de acesso em todas as contas
6. Hooks para integração com sistemas externos através de HTTP Post
7. Hooks para integração com sistemas externos, como Ticketing Systems
jj) O serviço proposto deve fornecer todas as funções de relatórios dentro do painel único do portal, sem a

necessidade de plataformas externas de relatórios.
kk) O serviço proposto deve incluir vários relatórios prontos para uso pré-configurados.
ll) O serviço proposto deve permitir que os relatórios integrados sejam personalizados diretamente a partir de um único painel, sem a necessidade de serviços profissionais do fornecedor.
mm) O serviço proposto deve fornecer a capacidade de gerar relatórios personalizados diretamente da interface de painel único sem a necessidadede serviços profissionais do fornecedor.
nn) O serviço proposto fornece uma trilha de auditoria para o fluxo de trabalho da conta de serviço e a aplicação da governança.
oo) Sessões Privilegiadas: o serviço proposto deve suportar a conexão transparente de um usuário do portal da Web a um recurso de destino por meio de RDP, SSH ou aplicativo.
pp) O serviço proposto deve suportar o monitoramento de uma sessão sem notificar o usuário conectado.
qq) O serviço proposto deve suportar o envio de uma mensagem ao usuário conectado.
rr) O serviço proposto deve oferecer suporte ao encerramento de uma sessão de usuário ativa.
ss) O serviço proposto deve fornecer aplicativos pré-configurados para o lançamento da sessão (RDP, SSH, PowerShell, SSMS, etc.).
tt) O serviço proposto deve fornecer a capacidade de adicionar nativamente inicializadores de sessão de aplicativos personalizados para serem configurados a partir de um único painel sem a necessidade de serviços profissionais de fornecedores.
uu) O serviço proposto não deve exigir aplicativos de middleware como AutoIt, AutoHotkey ou outras plataformas de automação de GUI do Windows para adicionar inicialização de sessão de aplicativo personalizado.
vv) O serviço proposto deve suportar o lançamento de sessões sem divulgação da senha.
ww) O serviço proposto deve suportar o registo automático de sessões com e sem notificação ao utilizador.
xx) O serviço proposto deve suportar a captura de eventos do aplicativo Windows durante as sessões.
yy) O serviço proposto deve oferecer suporte à pesquisa cruzada para processos executados do Windows, por exemplo, abrindo o PowerShell ou MMC.
uu) O serviço proposto deve fornecer um agente de gravação baseado em agente para capturar sessões do Windows. O agente deve permitir sessões de gravação iniciadas fora da plataforma PAM.
zz) O serviço proposto deve fornecer um método de agregação dos agentes de gravação em coleções lógicas.
aaa) O serviço proposto deve fornecer um método de lista de permissões de comandos emitidos para recursos baseados em SSH.
bbb) O serviço proposto deve suportar o descarregamento de gravações para um SAN, NAS ou outros compartilhamentos de rede enquanto ainda está sendo criptografado.
ccc) O serviço proposto deve suportar uma configuração em que as sessões RDP e SSH são intermediadas por meio do componente "jumpbox" do PAM. Descreva como esse fluxo de trabalho é realizado e quais componentes de arquitetura são necessários.
ddd) O serviço proposto deve suportar uma configuração em que as sessões RDP & SSH não requeiram um componente "jumpbox" para facilitar as conexões. Por favor, descreva como isso é feito.
eee) Se o serviço proposto tiver um componente "jumpbox", ela deverá suportar balanceamento de carga automático e failover automatizado sem Windows Server Failover Clusters.
fff) Descoberta de Contas: O serviço proposto deve incluir uma função automatizada de descoberta de contas.
ggg) A função de descoberta de conta do serviço proposto deve permitir o agendamento de hora em hora.
hhh) A função de descoberta de contas do serviço proposto deve fornecer uma exibição de resultados de descoberta fácil de entender para visualizar contas em todo o ambiente.
iii) A função de descoberta de contas de soluções propostas deve fornecer suporte pronto para uso para contas do Active Directory, contas do Windows, contas do Linux, contas do Unix, contas do Hypervisor.

jjj) A função de descoberta de contas do serviço proposto deve oferecer suporte a regras para automatizar a integração de todas as contas descobertas.
kkk) A função de descoberta de conta do serviço proposto deve ser extensível a outras plataformas não suportadas de fábrica. Descreva em detalhes como sua plataforma pode atender a esse requisito.
lll) A descoberta de conta do serviço proposto fornece a capacidade de descobrir contas de serviço e aplicar governança e propriedade.
mmm) API e Integração: O serviço proposto deve oferecer uma extensa API de serviços da Web com funções de criação, leitura, atualização e exclusão.
nnn) A API de serviços da Web do serviço proposto deve oferecer suporte à Autenticação Integrada do Windows e à Autenticação OAuth.
ooo) A API de serviços da Web do serviço proposto deve oferecer suporte à lista de permissões de endereços IP.
ppp) O uso da API de web services do serviço proposto deve ser auditável pela plataforma PAM.
qqq) O serviço proposto deve oferecer um SDK ou bibliotecas de programação para inclusão no código-fonte do software desenvolvido internamente.
rrr) As bibliotecas/SDK do serviço proposto devem oferecer suporte à lista de permissões de endereços IP.
sss) Os SDK/bibliotecas do serviço proposto devem ser auditáveis pelaplataforma PAM.
ttt) O cliente SDK ou CLI do serviço proposto deve oferecer uma estratégia de cache criptografada configurável.
uuu) A auditoria do cliente SDK ou CLI do serviço proposto deve estar acessível na plataforma.
vvv) O SDK do serviço proposto, o cliente CLI ou outros componentes da API não devem ser baseados em Java.
www) O serviço proposto deve fornecer uma interface/conector SCIM para integração em plataformas IdAM.
xxx) O serviço proposto deve ter uma integração direta com soluções comuns de varredura de vulnerabilidade (Nessus, Rapid7, Qualsys) para descarregar credenciais necessárias em varreduras autenticadas.
yyy) O serviço proposto suporta integração pronta para uso com sistemas de tiquetes comuns (ServiceNow, BMC, JIRA) para uso em validações de fluxo de trabalho.
zzz) Liste os pontos de integração das soluções propostas ou a metodologia de integração.
aaaa) O serviço proposto deve proteger os dados em movimento.
bbbb) O serviço proposto deve fornecer um relatório de auditoria do usuário; permitindo que os administradores visualizem quais contas um indivíduo excluído tocou.
cccc) O serviço proposto deve fornecer um método fácil para rotacionar as contas divulgadas no relatório de auditoria do usuário mencionado anteriormente.
dddd) O banco de dados MS SQL dO serviço proposto deve suportar MS Transparent Data Encryption. eeee)O serviço proposto deve suportar o descarregamento do gerenciamento da chave mestra de criptografia para um HSM (Hardware Security Module).
ffff) O serviço proposto deve oferecer uma função integrada de backup agendado capaz de salvar em uma SAN, NAS ou outro local de rede.
gggg) O serviço proposto deve suportar mensagens de erro de divulgação de informações zero para evitar que os logs exibam informações confidenciais.
hhhh) O serviço proposto deve suportar configuração para permitir portas fora do padrão.
iiii) O serviço proposto deve suportar um mecanismo de políticas de regras e complexidade de senha personalizável.
jjjj) O serviço proposto deve permitir que objetos de política de grupo organizacionais padrão sejam aplicados em todos os componentes da arquitetura da plataforma.
kkkk) O serviço proposto deve oferecer suporte à verificação de violações de segurança conhecidas de sites cujos logins são armazenados no gerenciador de senhas, para os quais você não alterou sua senha desde a ocorrência

da violação.
llll) Experiência do Usuário: O serviço deve fornecer uma interface de painel único para todos os acessos e configurações para todas as funções, por exemplo, administração, auditoria, geração de relatórios, proteção, políticas de acesso, sessões privilegiadas, descoberta e API.
mmmm) O serviço não deve exigir plug-ins de navegadores (Flash, Java, etc.) para qualquer função de acesso, inicialização, revisão, administração ou gerenciamento.
nnnn) A experiência do usuário do serviço proposto deve ser a mesma para todos os usuários, mas restrita por funções e permissões para agilizar o treinamento e a adoção.
oooo) A administração do serviço proposto e a experiência do usuário devem ser intuitivas.
pppp) A segregação de contas do serviço proposto deve imitar um explorador de sistema de arquivos de sistemas para simplificar o treinamento e aadoção.
qqqq) A hierarquia de segregação de contas do serviço proposto deve suportar um modelo de herança para recursos e políticas.
rrrr) A proposta deve fornecer um console de gerenciamento para gestão do ciclo de vida da conta de serviço que ofereça suporte à funcionalidade do solicitante/aprovador.
tttt) Gestão de Sessões: O serviço deve ser capaz de gerenciar e interagir com várias sessões remotas para protocolo de área de trabalho remota (RDP) e SSH em um ambiente unificado.
uuuu) O serviço deve ser capaz de gerenciar várias sessões ativas ao mesmo tempo, usando diferentes protocolos de conexão e uma variedade de contas privilegiadas.
vvvv) O serviço deve ser capaz de iniciar e configurar sessões em vários ambientes com credenciais injetadas automaticamente nas sessões conforme necessário.
wwww) O serviço deve ser capaz de fornecer um registro de ponta a ponta do acesso privilegiado do usuário e fornecer uma colaboração entre as equipes para visualizar ao vivo e enviar mensagens.
xxxx) O serviço deve fornecer banners de terminal personalizados após um login bem-sucedido exibindo os comandos disponíveis.
yyyy) O serviço deve ter a capacidade de iniciar uma conexão de terminal usando uma única linha e incluir 2FA para acesso.
zzzz) O serviço deve ser capaz de utilizar recursos integrados, como as setas para cima e para baixo para o histórico de comandos.
aaaaa) O serviço não deve exigir mais hardware ou licenciamento adicional para esses recursos de conexão de terminal.

2.6.3. REQUISITOS DE SERVIÇO

a) Segurança de Acesso: Um serviço de cofre de senha garante a segurança e o controle de acesso às senhas e informações confidenciais da CONTRATANTE, permitindo que apenas usuários autorizados possam visualizar e gerenciar esses dados.
b) Gerenciamento Centralizado: O serviço oferece armazenamento e gestão de senhas, eliminando a necessidade de senhas compartilhadas por e-mail ou armazenadas em documentos não seguros. Isso simplifica o gerenciamento de senhas e melhora a eficiência operacional.
c) Controle de Auditoria: O serviço registra todas as atividades relacionadas ao acesso e uso das senhas, permitindo uma trilha de auditoria detalhada. Isso ajuda a garantir a conformidade com as regulamentações de segurança e privacidade de dados, além de fornecer visibilidade sobre quem acessou as senhas e quando.
d) Compartilhamento Seguro: O serviço permite o compartilhamento seguro de senhas entre usuários autorizados, sem a necessidade de divulgar diretamente as senhas. Isso garante que as senhas sejam compartilhadas com segurança, minimizando o risco de exposição ou uso indevido.

e) Recuperação de Senha: O serviço oferece recursos de recuperação de senha para evitar perda de acesso a contas e sistemas críticos. Isso ajuda a minimizar interrupções operacionais e garantir a continuidade dos negócios.
f) Autenticação Multifator: O serviço de cofre de senha suporta autenticação multifator, adicionando uma camada extra de segurança ao acesso às senhas, ajudando a proteger as informações confidenciais contra acesso não autorizado.
g) Gerenciamento de Credenciais: O serviço de PAM permite o gerenciamento centralizado de credenciais privilegiadas, como senhas e chaves de acesso, para contas de administradores, sistemas, dispositivos e aplicativos. Isso ajuda a evitar senhas compartilhadas, facilita a rotação regular de senhas e garante o acesso seguro a recursos críticos.
h) Controle de Acesso Granular: Com o serviço de PAM, é possível definir políticas de acesso detalhadas para usuários privilegiados, limitando o acesso apenas às informações e recursos necessários para suas funções. Isso reduz o risco de uso indevido ou abuso de privilégios.
i) Auditoria e Monitoramento: O serviço de PAM registrará e monitorará todas as atividades dos usuários privilegiados, incluindo registros de acesso, comandos executados e alterações feitas. Isso fornece uma trilha de auditoria completa e ajuda na detecção de atividades suspeitas ou não autorizadas.
j) Gerenciamento de Sessões: O serviço de PAM permitirá o controle e o monitoramento das sessões de acesso privilegiado em tempo real. Ele possibilita o início, o término e a gravação de sessões, além de permitir a visualização em tempo real das atividades realizadas durante as sessões.
k) Autenticação Multifator (MFA): o serviço de PAM oferecerá suporte a autenticação multifator, adicionando uma camada extra de segurança ao exigir que os usuários privilegiados forneçam mais de uma forma de autenticação, como senha, token físico ou biometria.
l) Gestão de Políticas: O serviço de PAM permitirá a criação e a aplicação de políticas de segurança consistentes para acesso privilegiado. Isso incluirá definir requisitos de senha, tempo de expiração, restrições de uso e outras políticas de conformidade.
m) Privacidade e Isolamento: O serviço PAM garantirá a privacidade e o isolamento de credenciais privilegiadas, protegendo-as contra acesso não autorizado, alcançado por meio de técnicas como criptografia, armazenamento seguro e segregação de funções.
n) Integração com Outras Soluções de Segurança: O serviço de PAM oferecerá integração com outros sistemas de segurança, como SIEM (Security Information and Event Management), sistemas de gerenciamento de identidade e acesso (IAM) e soluções de gerenciamento de vulnerabilidades.

2.6.4. REQUISITOS DE COMUNICAÇÃO

a) Sempre que solicitado pela CONTRATANTE a CONTRATADA deverá por e-mail ou outro meio estabelecido previamente, deverá ser entregue um relatório em português sobre status do serviço, com métricas e sugestões de melhoria, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas;
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
e) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
f) É responsabilidade da CONTRATADA supervisionar as rotinas de backup e restauração dos equipamentos,

softwares e configurações implantadas referentes a segurança da informação;
g) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobrea criação ou atualizações de tiquetes.
h) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
i) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da contratada.
j) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.

2.6.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) O serviço deve ser compatível com diferentes plataformas e sistemas operacionais, como Windows, macOS, Linux, Android, iOS, entre outros.
b) Deve ser integrável com o Diretório Ativo (Active Directory) ou outros sistemas de autenticação baseados em LDAP, permitindo a sincronização desenhas de forma centralizada.
c) O serviço deve ser capaz de integrar-se com aplicações e serviços em nuvem, como G Suite, Office 365, Salesforce, entre outros, para facilitar o gerenciamento de senhas.
d) Deve suportar protocolos de autenticação padrão, como SAML, OAuth e OpenID Connect, para permitir uma autenticação segura e eficiente.
e) Deve ser integrável com soluções de Single Sign-On para proporcionar uma experiência de login única para os usuários em diferentes sistemas.
f) O serviço deve fornecer APIs bem documentadas e web services para permitir a integração com outros sistemas e possibilitar a automação de tarefas.
g) O serviço deve ser integrável com plataformas de IAM para sincronizar as informações de usuários e senhas de forma segura.
h) Deve ser possível integrar os logs e eventos do serviço de gestão de senhas com ferramentas de segurança e SIEM para monitoramento e análise continua.
i) Deve ser compatível com gerenciadores de senhas de navegadores populares para facilitar o preenchimento de credenciais de forma segura.
j) Deve suportar a integração com soluções de autenticação multifator para aumentar a segurança das contas dos usuários.
k) Deve ser integrável com ferramentas de gerenciamento de vulnerabilidades para acompanhar a segurança das senhas em relação às ameaças conhecidas.

2.6.6. REQUISITOS DE ATIVAÇÃO

a) O serviço deve ser ativado em um ambiente de hospedagem adequado, com a infraestrutura necessária para suportar o tráfego e o armazenamento seguro das senhas.
b) Deve haver um levantamento claro dos requisitos de sistema, incluindo capacidade de processamento, memória, armazenamento e largura de banda para garantir o desempenho adequado do serviço.
c) O serviço de gestão de senhas deve ser compatível com as plataformas e sistemas operacionais que o DETRAN-PA utiliza, garantindo a facilidade de uso e a adoção pelo usuário.
d) A ativação do serviço deve garantir o acesso controlado por usuários autorizados, utilizando autenticação segura e privilégios de acesso adequados.
e) Deve ser implementado um sistema de backup regular dos dados do serviço, permitindo a recuperação em caso

de perda de informações.
f) O serviço de gestão de senhas deve passar por testes rigorosos de validação antes da instalação, garantindo sua estabilidade e funcionalidade.
g) O serviço deve ser configurado de acordo com as necessidades específicas do DETRAN-PA, incluindo políticas de senha, regras de acesso e integrações com sistemas existentes.
h) Deve ser realizada a integração com os sistemas e aplicativos existentes da organização, garantindo a sincronização das senhas e uma experiência de usuário coesa.
i) O serviço deve oferecer recursos de auditoria e conformidade, permitindo rastrear atividades relacionadas ao gerenciamento de senhas para fins de segurança e conformidade.
j) A ativação do serviço deve estar em conformidade com as regulamentações e leis aplicáveis relacionadas à privacidade e segurança de dados.

2.7. SERVIÇO DE ACESSO SEGURO REMOTO ZTNA

2.7.1. REQUISITOS DE NEGÓCIO

a) O Serviço deve oferecer acesso seguro a recursos de rede com base no modelo Zero Trust, permitindo conexões somente a usuários autorizados, independentemente da localização da rede.
b) O serviço deverá oferecer aos usuários remotos a capacidade de acessar recursos de rede de forma segura, independentemente de sua localização.
c) Isso será alcançado através da criação de túneis criptografados que protegem o tráfego entre o usuário e os recursos da rede interna.
d) O Serviço deve oferecer autenticação multifator (MFA) para todos os usuários, garantindo a identidade e minimizando o risco de acesso não autorizado.
e) O Serviço deve permitir a definição de políticas de acesso granulares, garantindo que apenas os usuários autorizados tenham acesso a recursos específicos.
f) O Serviço deve estabelecer conexões seguras entre usuários remotos e recursos de rede, utilizando criptografia robusta para proteger os dados em trânsito.
g) O Serviço deve oferecer suporte a diversos protocolos de rede para acomodar diferentes tipos de aplicativos e serviços.
h) O Serviço deve ser capaz de identificar padrões de comportamento incomuns que possam indicar atividades maliciosas.
i) O Serviço deve ser dimensionável para acomodar um grande número de usuários e conexões simultâneas, mantendo o desempenho adequado.
j) O Serviço deve oferecer suporte a uma ampla variedade de aplicativos e serviços, incluindo aplicativos baseados em nuvem, aplicativos locais e serviços web.
k) O Serviço deve ser capaz de integrar-se de forma harmoniosa com a infraestrutura de TI existente, incluindo sistemas de autenticação, diretórios de usuários e sistemas de monitoramento.
l) O Serviço deve estar em conformidade com as regulamentações de segurança e privacidade relevantes, garantindo que os dados do usuário sejam protegidos adequadamente.
m) O Serviço deve fornecer atualizações regulares de segurança e manutenção para proteger contra vulnerabilidades conhecidas e melhorar a eficácia geral da plataforma.
n) O Serviço deve ser altamente disponível, minimizando o tempo de inatividade planejado e não planejado, e deve incluir mecanismos de redundância para garantir a continuidade do serviço.

2.7.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES

a) Deve ter a capacidade de usar Inteligência Artificial e Machine Learning para detectar o uso de aplicativos

maliciosos e o acesso pelo usuário, permitindo que sejam bloqueados.
b) O Gateway deve seguir o conceito baseado em nuvem, permitindo o controle e inspeção de acesso a aplicativos SAAS tradicionais e aplicativos locais, eliminando a necessidade de uma VPN tradicional.
c) Habilitar controle granular de aplicativos e integração total com o sistema antivírus do End Point.
d) Deve possuir um Engine baseado em Inteligência Artificial e hospedado na nuvem que permita um processo contínuo de autenticação contínua dos usuários de acordo com o perfil de uso do aplicativo. E ser capaz de detectar anomalias continuamente e, se possível, solicitar a autenticação do usuário.
e) Para aplicações On Premises, o serviço deve fornecer um conector que permita estabelecer comunicação segura e eficiente entre o ambiente LAN local onde residem as aplicações e o Gateway presente na nuvem.
f) O serviço deverá apresentar um conjunto de fatores para verificar o nível de risco e se o usuário é confiável, incluindo:
1. A localização e o IP do usuário são seguros,
2. Processo contínuo de autenticação do usuário, que pode incorporar autenticação de dois fatores,
3. Hora e dia da semana em que ocorre o acesso, podendo assim identificar anomalias na utilização das aplicações fora do horário de trabalho,
4. Se o usuário estiver acessando arquivos e dados que normalmente acessa,
5. Se o comportamento do usuário for consistente e semelhante ao de outros usuários da empresa,
g) Dependendo do nível de risco encontrado, a solução deve ser capaz de realizar automaticamente as seguintes ações:
1. Garantia de acesso
2. Negar acesso
3. Adaptar a política de acesso
4. Alertar apenas para que uma equipe de remediação possa agir
h) Deverá permitir trabalhar no modo Full Tunnel e Split Tunnel
i) Deverá possui capacidade de configuração de IP de origem
j) Deve ser integrado ao console de gerenciamento da solução EDR e End Point Protection
k) Permitir que o tráfego do Office 365 seja descarregado diretamente no Gateway sem a necessidade de passar pela rede local
l) Permitir acesso remoto Zero Trust a aplicativos ON Prem
m) Forneça autenticação continua incorporando a capacidade de usar autenticação multifator
n) Para impedir que os usuários acessem sites de má reputação e sites maliciosos, essas regras devem permitir uma configuração granular
o) Permitir a criação de regras para que o tráfego específico de baixa latência seja enviado diretamente para a Internet sem passar pelo Gateway
p) Correlacionar dados de telemetria de rede de endpoint, permitindo assim que atividades maliciosas de malware sejam mapeadas para tráfego suspeito.
q) Investigar eventos anômalos relacionados a ameaças e vulnerabilidades
r) Tenha painéis gráficos onde você pode rastrear o tráfego de rede e as ações do usuário
s) Os alertas devem conter no mínimo as seguintes informações:
1. Descrição
2. Nível de risco: alto, médio e baixo
3. Tipo de evento
4. Data e hora da detecção
5. Dispositivo afetado
6. Usuário afetado

7. Política aplicada para resposta
t) Deve permitir a criação de políticas granulares de acordo com o nível de risco encontrado no incidente.
u) Deve permitir a priorização de políticas para que as políticas de maior prioridade sejam abordadas primeiro.
v) Deve permitir que a filtragem da web continue a funcionar, apesar dos usuários interromperem o serviço.
w) Deve permitir a fixação de endereço IP para que todo o tráfego roteado para o Gateway para um determinado servidor de destino use um endereçou intervalo IP específico.
x) Deve permitir o uso de múltiplos conectores para facilitar a integração com aplicações locais localizadas em diferentes redes ou localidades.
y) Deve ter um mecanismo IPS, para que possa bloquear o tráfego malicioso em tempo real.
z) Deve possuir um filtro web integrado, que permita o bloqueio de páginas web por categoria ou de forma granular.

2.7.3. REQUISITOS DE SERVIÇO

a) A CONTRATANTE espera que o serviço de ZTNA seja operada por engenheiros certificados e analistas de segurança experientes de SOCs 24 horas por dia, 7 dias por semana.
b) A detecção, análise e relatórios detalhados de incidentes de segurança de ataques cibernéticos devem ser fornecidos por do serviço de ZTNA.
c) A CONTRATADA deve fornecer toda a infraestrutura tecnológica e os recursos necessários para a implantação e operação da plataforma ZTNA.
d) A CONTRATADA deverá possuir e disponibilizar uma interface central para visualizar todas as regras e o status das aplicações na plataforma ZTNA.
e) A CONTRATADA deve fornecer todas as soluções tecnológicas e serviços necessários para garantir a execução do serviço.
f) A CONTRATANTE deve ter acesso a um painel de controle no serviço de ZTNA para gerenciar determinadas configurações quando considerar apropriado.

2.7.4. REQUISITOS DE COMUNICAÇÃO

a) Sempre que solicitado pela CONTRATANTE a CONTRATADA deverá por e-mail ou outro meio estabelecido previamente, deverá ser entregue um relatório em português sobre status do serviço, com métricas e sugestões de melhoria, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas;
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobre a criação ou atualizações de tiquetes.
e) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
f) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da contratada.
g) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da

CONTRATADA por telefone.

2.7.5. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) Deve estar acessível, com versões compatíveis tanto para Windows 10 quanto para dispositivos móveis Android e iPhone, integrando-se ao sistema antivírus dessas plataformas.

b) Deve ser integrável com o Diretório Ativo (Active Directory) ou outros sistemas de autenticação baseados em LDAP, permitindo a sincronização desenhas de forma centralizada.

c) O serviço deve ser capaz de integrar-se com aplicações e serviços em nuvem, como G Suite e Office 365.

d) Deve suportar protocolos de autenticação padrão, como SAML, OAuth e OpenID Connect, para permitir uma autenticação segura e eficiente.

2.8. SERVIÇO DE CONSULTORIA ESPECIALIZADA EM CIBERSEGURANÇA ASSESSMENT

2.8.1. REQUISITOS DE NEGÓCIO

a) A CONTRATANTE busca serviços de consultoria em segurança da informação, para trazer maior proteção aos colaboradores, bem como os clientes atendidos pela CONTRATANTE.

b) Devem ser utilizadas as ferramentas de segurança da CONTRATADA e da CONTRATANTE para realização do serviço de consultoria.

c) Conforme definição da CONTRATANTE, a CONTRATADA deverá ser responsável pelo Serviço de Consultoria para Melhoria Operacional da Segurança da Informação e apoio com ações Evolutivas e Corretivas.

d) Deve ser contemplada serviço de consultoria em modelo de banco de horas.

e) O serviço deverá ser realizado localmente, caso a CONTRATANTE julgue necessário poderá eventualmente definir que seja realizado remotamente.

2.8.2. CARATERÍSTICAS GERAIS DO SERVIÇO DE CONSULTORIA

a) A CONTRATADA deverá realizar, através de serviços de consultoria, ajustes e recomendações relacionados aos processos e padrões especificados pela CONTRATANTE.

b) Como parte de qualquer organização que possui iniciativas de melhoria da segurança da informação, é sempre recomendável, e na maioria dos casos, rever o estado atual da arquitetura de segurança e compreender a necessidade de melhoria necessária para permitir que a organização elabore um plano de ação que garanta a adequação continuada da gestão de riscos, além de manter a conformidade com regulamentações externas e mandatos contratuais.

c) Para atingir estes objetivos, a CONTRATADA desenvolverá um processo de avaliação para ajudar a CONTRATANTE a avaliar de forma global os processos e a arquitetura da segurança da informação da sua CONTRATANTE e identificar áreas específicas que precisam ser melhoradas. Baseado em melhores práticas de mercado, e na experiência prática e conhecimento da indústria de tecnologia, esta avaliação de segurança da informação deverá fornecer a educação e orientação necessária para entender e começar a aplicar ações de governança corporativa de segurança.

d) O principal objetivo das horas de consultoria será acelerar e apoiar a CONTRATANTE na adoção dos serviços gerenciados de segurança e garantir o aumento do nível de maturidade de todo o ciclo de vida de incidentes, atuando com um olhar crítico a partir da visão da CONTRATANTE, agregando a experiência dos consultores da CONTRATADA e as melhores práticas de mercado.

e) Deverá ser estabelecida em conjunto, CONTRATADA e CONTRATANTE, as prioridades dos serviços de consultoria, assim que definido o plano de trabalho as atividades consultivas de cibersegurança poderão ser realizadas.

f) As horas contratadas para consultoria devem ser consumidas através das seguintes atividades, exclusivamente:

1. Identificação, desenvolvimento, implementação e manutenção de processos corporativos
2. Monitoramento do plano de resposta a incidentes
3. Apoio para construção/readequação na arquitetura de segurança
4. Condução de GAP Analysis de Segurança e frameworks específicos
5. Identificação de oportunidades para melhorias no ambiente (Estratégias, Serviços, Plataformas)
6. Análise de Riscos de Segurança
7. Políticas e Procedimentos
8. Treinamento de conscientização dos usuários em segurança cibernética

2.8.2.1. IDENTIFICAÇÃO, DESENVOLVIMENTO, IMPLEMENTAÇÃO E MANUTENÇÃO DE PROCESSOS CORPORATIVOS

A CONTRATADA deverá utilizar-se de frameworks como o NIST Cyber Security Framework, CIS Controls, ISA/IEC 62443, juntamente com os padrões de segurança da série ISO/IEC 27000, como uma base para transmitir as pessoas adequadas, processos e tecnologia necessários para suportar o ciclo de vida da segurança dentro da CONTRATANTE e auxiliar na manutenção dos processos corporativos com foco em segurança.

2.8.2.2. MONITORAMENTO DO PLANO DE RESPOSTA A INCIDENTES

a) O serviço a ser prestado deverá exigir uso das ferramentas necessárias para suportar o controle de alterações e rastrear ativos com base na sua estrutura de classificação.

b) Quando ocorre um incidente, o serviço deverá possuir requisitos que monitorem e rastreiem incidentes e forneçam recursos para dar suporte ao processo implementado.

c) Desenvolver uma política de resposta a incidentes, incluindo um processo de resposta a incidentes.

2.8.2.3. APOIO PARA CONSTRUÇÃO/READEQUAÇÃO NA ARQUITETURA DE SEGURANÇA

Consultoria para apoio na Arquitetura de Segurança Lógica e Modelo de Domínio de Segurança com a Estrutura de Classificação de Segurança da Informação com abordagem em camadas de defesa profunda, baseada em:

1. Conjunto de controles para a classificação de domínio.
2. Nível de isolamento por domínio.
3. Controles técnicos e não técnicos nos níveis de Operações, Aplicações, Terminais e Infraestrutura.

2.8.2.4. CONDUÇÃO DE GAP ANALYSIS DE SEGURANÇA E FRAMEWORKS ESPECÍFICOS

Consultoria para apoio de GAP Analysis para frameworks específicos conforme a necessidade.

2.8.2.5. IDENTIFICAÇÃO DE OPORTUNIDADES PARA MELHORIAS NO AMBIENTE (ESTRATÉGIAS, SERVIÇOS, PLATAFORMAS)

a) Apoio de consultoria para recomendações de novas soluções, serviços e adequações na operação conforme evolução da área de segurança.

b) Elaborar e atualizar documentações e procedimentos necessários para administração, operação e suporte do ambiente gerenciado, garantindo sua atualização sempre que necessário.

2.8.2.6. ANÁLISE RISCOS DE SEGURANÇA

a) Realização de Risk Analysis associado a vulnerabilidades encontradas em ambientes de IT (Análise de Vulnerabilidades Tecnológicas) e com os resultados da Análise de Conformidade.

b) A metodologia e framework utilizado para o serviço de Análise de Riscos em Segurança deve ser a ISO/IEC 27005.

c) Sua abordagem e metodologia devem ser usadas em combinação com outros padrões de segurança de TI, como a série ISO 27000 que tem o foco em:
1. Confidencialidade (C), Integridade (I), Disponibilidade (A)
2. Sistema de gerenciamento de segurança da informação (SGSI)
3. Classificação de informações, análise de riscos, conceito de segurança
4. Abordagem Plan-Do-Check-Act para segurança de TI
d) Entregáveis:
1. Relatório Executivo (Riscos mapeados, Controles encontrados, Recomendações, Riscos Residuais)
2. Planilha Técnica (Matriz de Riscos, Vulnerabilidades, Impacto, Ameaças, Ativos, Controles, Ricos Atuais X Riscos Residuais, Probabilidade).

2.8.2.7. POLÍTICAS E PROCEDIMENTOS

a) Confecção de políticas e procedimentos de segurança cibernética devendo cobrir com detalhes temas como:
1. Desenvolvimento Seguro
2. Segurança em Recursos Humanos
3. Gestão de Prestadores de Serviços e Parceiros
4. Gestão de Ativos
5. Criptografia
6. Política Geral de Segurança Informação
7. Programa de Conscientização de Segurança da Informação Uso Aceitável
8. Privacidade de Dados Pessoais
9. Perímetros de Segurança Eletrônica
10. Resposta a Incidentes
11. Gerenciamento de Mudanças

2.8.2.8. FORMA DE TRABALHO

A abordagem da CONTRATADA à segurança da informação deverá ser "TOP-DOWN", ou seja, alinhada aos negócios para fornecer rastreabilidade e justificativa para controles de segurança - técnicos e não técnicos. As práticas de segurança da informação e gestão de risco devem ser simples, apropriadas e economicamente proporcionais para garantir que o esforço e os recursos sejam empregados de acordo. Essa abordagem holística à segurança da informação garante conformidade com todos os padrões e estruturas de melhores práticas, além de influências internas e externas de segurança. Essas metodologias comprovadas apresentam arquiteturas sólidas de segurança para proteger contra as ameaças mais recentes e avançadas, ao mesmo tempo em que fornecem ambientes ágeis e flexíveis que permitem e suportam iniciativas de negócios.

2.8.2.9. ESCOPO CONSULTIVO

A CONTRATANTE entende que um Banco de Horas de até 4.000 (quatro mil) horas ao longo dos 12 (doze) meses, para consumir com os serviços da CONTRATADA de serviços de consultoria para realizar estes ajustes, proposições, acompanhamentos de roadmaps e atualização de documentações para a CONTRATANTE seja suficiente. A CONTRATANTE não se compromete a um consumo mínimo de horas e pode não contratar este item.

2.8.2.10. INTERPRETAÇÃO DA ARQUITETURA DE SEGURANÇA DA INFORMAÇÃO

a) As seguintes exibições de arquitetura em camadas, conforme definidas pelo SABSA1, apresentam segurança de informações corporativas holísticas e deverão ser consideradas em nossos contratos de arquitetura:

FIGURA VISÃO DA ARQUITETURA DE SEGURANÇA, COMO DEFINIDO PELA SABSA

b) As arquiteturas de segurança técnica devem apresentar controles que gerenciam os riscos identificados, alinhados a um conjunto de políticas voltadas para os negócios (para cada domínio de risco), para permitir a governabilidade. Quando as políticas não existem para orientar arquiteturas de segurança técnica, elas devem, pelo menos, seguir as práticas recomendadas do setor para garantir que os riscos comuns e fundamentais possam ser identificados e gerenciados.

c) Do ponto de vista lógico, não importa realmente como os controles físicos e de componentes deverão ser aplicados ou quais fornecedores e tecnologias deverão ser usados, desde que atendam aos requisitos definidos pelas três primeiras camadas de arquitetura de segurança: contextual, conceitual e lógica.

d) Essa abordagem garante a repetibilidade e a consistência usando uma metodologia que apresenta segurança dinâmica e adaptativa que suporta e permite todas as iniciativas de negócios, incluindo Cloud, Enterprise Mobility e BYOD.

e) A segurança por si só não tem sentido. A obtenção desse direito garante longevidade e relevância para os negócios, a fim de possibilitar oportunidades com segurança e gerenciar riscos de acordo com um apetite de risco apropriado.

2.8.3. PREMISSAS GERAIS

a) Os serviços deverão ser executados a partir das localidades de trabalho do SOC (Centro de Operações de Segurança) e Serviço Gerenciado de Segurança da CONTRATADA.

b) Estes serviços deverão ser executados em modelo 8x5xNBD.
c) Entende-se por horário de atendimento 8x5xNBD de segunda a sexta, a partir de 08:00 até às 17:00.
d) A CONTRATANTE fornecerá todas as informações necessárias para execução do serviço e tomada de decisão sobre um determinado item, tentando, ao máximo, seguir a recomendação e expertise da CONTRATADA.
e) O serviço deverá ser realizado localmente, caso a CONTRATANTE julgue necessário poderá eventualmente definir que seja realizado remotamente.

2.9. SERVIÇO DE NETWORK DETECTION AND RESPONSE – NDR
2.9.1. REQUISITOS DE NEGÓCIO
a) O fornecimento do serviço será realizado através de um Centro de Operações de Segurança (Security Operation Center - SOC) pertencente à CONTRATADA.
b) O Serviço de NDR será disponibilizado para ser usado na infraestrutura de rede da CONTRATANTE, bem como todos os itens necessários, hardware e software, para a realização dos serviços.
c) A abordagem dos serviços, deverá ser baseada na suposição de que a ameaça já se encontra dentro do ambiente organizacional, utilizando o tráfego de rede como fonte para identificar possíveis rastros deixados.
d) Será viabilizada a implantação, pela organização, de um procedimento de investigação, busca por ameaças e análise forense de rede, empregando metadados da solução com funcionalidades de detecção e investigação.
e) O serviço será prestado à equipe da CONTRATANTE e ao serviço de SOC para realizar a triagem e investigação dos eventos de rede, com o objetivo de identificar comportamentos maliciosos mais complexos.
f) Será possível aos analistas de segurança realizar a triagem e investigação dos eventos de rede, elaborando consultas a partir dos resultados anteriores, com o intuito de identificar comportamentos maliciosos sofisticados.
g) A alimentação do sistema, disponibilizado para o serviço, ocorrerá através de múltiplas fontes de inteligência de ameaças, incluindo pesquisas internas, fontes comerciais, comunidades Open Source e entidades especializadas de setores específicos, como indústria e governo.
h) O serviço deve garantir o desempenho mesmo diante do grande volume de dados coletados, processados e armazenados.

2.9.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES
a) O serviço deverá identificar de forma autônoma, sem intervenção humana, todas as redes ativas no ambiente (que tiveram tráfego inspecionado) e apresentar uma relação com todas as redes, máscara de rede, primeira vez em que a rede foi observada e quantidade de dispositivos observados na rede correspondente.
b) O serviço deverá identificar de forma autônoma, sem intervenção humana, todos os endereços IPs que trafegaram nas redes inspecionadas apresentando uma relação com no mínimo os seguintes dados:
1. Classificação do tipo de dispositivo (desktop, servidor,Impressora, câmera, iot, etc)
2. IP do dispositivo
3. Mac Address
4. Nome DNS do dispositivo
5. Primeira vez que o dispositivo/IP foi visto na rede
6. Última vez que o dispositivo foi visto na rede
c) Deve ser possível visualizar o histórico de IPs de um determinado dispositivo baseado no IP provido pelo servidor DHCP.
d) O serviço deverá criar métricas, de forma autônoma, de raridade de Ips, Domínios DNS, Dispositivos, etc baseado na frequência que estes são acessados através da rede.
e) O serviço deverá criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio, etc contra as ações de mesmo escopo realizadas no passado.

1. A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.
f) O serviço deverá ser comprovadamente baseado em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:
1. Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados com por dispositivos da rede interna.
2. Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.
3. Dispositivo se comunicando com um servidor usando um certificado expirado.
4. Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.
5. Dispositivo iniciando várias conexões para um IP externo raro de maneira regular. (Beaconing)
6. Dispositivo gerando muitas solicitações para servidores Web internos o qual está retornando códigos de erro HTTP.
7. Novo dispositivo entrou na rede e começou a utilizar o software de teste de penetração ou escaneamento de rede.
8. Vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.
9. Dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS)
10. Dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.
11. Dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico.
12. Dispositivo gerando um volume anormalmente alto de solicitações DNS.
13. Dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.
14. Um servidor DNS interno está agindo como um resolvedor de DNSaberto (OpenDns).
15. Dispositivo se comunicando com o serviço de anonimização da redeTOR.
16. Dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.
17. Atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.
18. Dispositivo executando comandos PsExec em uma máquina remota que nunca havia recebido tráfego similar anteriormente.
19. Dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.
20. Dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.
21. Dispositivo fazendo conexões com hostnames raros associados a uma botnet.
22. Dispositivo solicitando um domínio conhecido por hospedar malwares.
23. Dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.
24. Dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.
25. Dispositivo fazendo download dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.
26. Dispositivo se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de SMB na rede interna.
27. Dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.
28. Dispositivo não conseguiu estabelecer uma sessão SMB2 seguida de uma configuração bem-sucedida da

sessão SMB1 usando credenciais administrativas.
29. Dispositivo lendo e gravando volumes de dados semelhantes para compartilhamentos de arquivos remotos.
30. Dispositivo acessando arquivos que possuem senhas não criptografadas.
31. Dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.
32. Dispositivo fazendo conexões web externas sem usar um proxy web.
33. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.
34. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.
35. Dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.
36. Dispositivo foi redirecionado para um Hostname HTTP raro e em seguida baixou um executável ou outro arquivo binário.
37. Dispositivo causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.
38. Dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.
39. Dispositivo informando no cabeçalho User-Agent que possui um sistema operacional o qual é diferente do SO que realmente está utilizando.
40. Dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.
41. Dispositivo fazendo download de arquivo executável vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.
42. Dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.
43. Dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.
44. Dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros.
45. Dispositivo enviando dados para o Pastebin.
46. Dispositivo usando um sistema terceiro de mensageria (Whatsapp ou similares).
47. Dispositivo acessando rede social (Facebook ou similares).
48. Dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.
49. Dispositivo fazendo conexões peer-to-peer BitTorrent.
50. Dispositivo recebeu um número anormalmente grande de conexões de entrada de IP externos raros.
51. Dispositivo fazendo conexões SQL para IPs externos a rede.
52. Dispositivo enviando uma quantidade anormal alta de dados paradestinos fora da rede.
53. Dispositivo trocando um volume de dados anormal com outrodispositivo na rede interna.
54. Dispositivo enviando uma quantidade anormalmente alta de dadosexternamente para um local para o qual a rede não enviou dados anteriormente.
55. Dispositivo explorado vulnerabilidade Heartbleed na rede interna.
56. Dispositivo se conectando a um DNS SinkHole conhecido.
57. Dispositivo realizando grandes volumes de pequenas conexões SSHe/ou RDP.
58. Dispositivo iniciando um grande número de conexões para umservidor RDP e/ou SSH.
59. Dispositivo recebendo um grande número de conexões RDP de entrada de IPs externos raros.
60. Alteração de bloco CIDR de uma subrede.
61. Alteração no comportamento de tráfego DHCP.
62. Novo servidor DNS na rede.

63. Novo servidor de proxy web na rede.
64. Adição ou remoção de domínios DNS na rede.
65. Perda de pacotes é superior a X% na rede.
66. Uma senha de credencial de alto privilégio foi alterada no domínio Windows.
67. Uma credencial efetuando login de uma origem incomum.
68. Uma credencial foi usada em múltiplos dispositivos internos.
69. Um dispositivo gerou um grande número de falhas de sessão SMB.
70. Um dispositivo desviou de suas atividades normais criando várias falhas de login Kerberos.

g) Deve ser possível criar regras utilizando um ou mais dos componentes do item acima.
h) Todos os dados processados devem ser armazenados para posterior análise independentemente de terem gerado alertas ou não.
i) O serviço deverá possuir mecanismos para exportar os dados armazenados no padrão de extensão '.pcap'.
j) Deve ser capaz de agrupar de forma autônoma dispositivos em grupos baseado em sua similaridade de comportamento.
k) Deve ser capaz de tomar ações baseadas em desvio de comportamento.
l) Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede.
m) Deve possuir a habilidade para responder, desacelerar e/ou parar ameaças autonomamente.
n) Deve ser capaz de marcar dispositivos automaticamente para decisões de resposta e ajuste fino.
o) Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede.
p) Deve ser capaz de registrar todas as ações de resposta para propósitos de auditoria.
q) Deve ser configurável para supervisão e aprovação de analistas em ações de tomada de decisão / resposta.

2.9.3. CARACTERÍSTICAS DE GERENCIAMENTO DA PLATAFORMA

a) O serviço deverá possuir controle de interface gráfica (GUI: Graphical User Interface) e interface texto (CLI);
b) A interface de texto (CLI) deve possuir comandos para permitir a realização de troubleshooting.
c) A interface gráfica não deve ser desenvolvida ou conter componentes baseados em java por questões de compatibilidade com browsers modernos.
d) A interface gráfica deve possuir no mínimo:
1. Sumário dos dados aprendidos como: Dados totais processados por dia, Quantidade de Redes, Dispositivos e usuários identificados na rede
2. Lista de alertas de anormalidade identificadas.
3. Critérios de filtro dos alertas de anormalidade por categoria de alerta, dispositivo ou usuários.
4. Critérios de filtro de período (data e horário) para os alertas de anormalidade.
5. Critérios de filtro de prioridade (risco) para os alertas de anormalidade.
6. Apresentar a posição geográfica das redes no ambiente de TI.
7. Opções de configuração do sistema
8. Área de gerenciamento de usuários
9. Área para gerenciamento de arquivos .pcap, exportação e visualização na própria interface.
10. Área de busca de dados na base de dados da solução.

e) Os alertas de anomalia devem conter no mínimo os seguintes dados:
1. Identificador único (Unique ID).
2. Data e horário.
3. Dispositivo que originou a ação.
I. Apresentar o IP de origem do Dispositivo.

II. Apresentar o MAC address do Dispositivo.
III. Apresentar o Hostname (DNS) do Dispositivo.
IV. Apresentar o (s) usuário(s) que se eventualmente se logaram no Dispositivo nas últimas horas.
V. Apresentar o a rede a qual o dispositivo estava conectado.
4. Descrição técnica do evento.
5. Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.
6. Atalho para acesso rápido às configurações da política que gerou o alerta.
7. Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta.
8. Atalho para acessar dados detalhados das ações que causaram a anomalia e subsequente alerta.
f) Durante a investigação de uma anomalia/alerta o administrador pode acessar os dados abaixo utilizando apenas o mouse.
1. Dados detalhados do dispositivo que originou a anomalia.
2. IP do dispositivo
3. Mac Address
4. Nome DNS do dispositivo
5. Primeira vez que o dispositivo/IP foi visto na rede
6. Última vez que o dispositivo foi visto na rede
7. Apresentar o (s) usuário(s) que se eventualmente se logou(aram) noDispositivo.
8. Apresentar a rede a qual o dispositivo estava conectado.
9. Acesso a todas as comunicações realizadas pelo dispositivo na rede.
10. Acesso a todas as anomalias as quais o dispositivo gerou na rede.
11. Acesso a ferramenta para geração de gráficos que facilitem a investigação utilizando critérios como, mas não limitados a:
I. Dados relacionados a conexões.
II. Tráfego de dados.
III. Requisições DNS.
IV. Erros de Login.
V. Ações utilizando SMB.
g) Apresentar gráfico representando os fluxos de comunicação entre os dispositivos que originaram e receberam tráfego anômalo.
h) O serviço deverá possuir mecanismo para automação de investigação de alertas permitindo a correlação entre múltiplos evento apresentando em uma única tela as seguintes informações:
1. Linha do tempo apontando a correlação entre alertas emitidos para um determinado dispositivo, data e horário em que cada alerta foi emitido bem como o período em que cada ação anômala, que gerou o alerta, ocorreu.
2. Apresentação individual de cada alerta contendo: Descrição do comportamento anômalo e riscos associados.
3. Dados técnicos relacionados ao alerta como:
I. Período em que a anomalia foi observada.
II. IP de origem
III. IP(s) de destino
IV. Credencial de usuário observada no dispositivo
V. Ação anômala identificada pela solução.
VI. Acesso aos logs do tráfego anômalo.
4. Deverá classificar cada alerta baseado em fases de ataque.
5. Deve permitir ao administrador exportar todas as informações acima em documento padrão .pdf.
i) A interface deve permitir a procura e navegação de qualquer dispositivo, usuário, Ips, etc que tenham sido

inspecionados em qualquer data armazenada pela solução.
j) Ao navegar pelas comunicações do dispositivo o administrador pode utilizar filtros baseados em IP, Porta e Protocolo para facilitar a visualização.
k) Ao navegar pelas comunicações do dispositivo o administrador pode utilizar um IP de destino como filtro permitindo a investigação de 'Origem > Destino' ou 'Destino > Origem'.
l) Ao navegar pelas comunicações de um usuário o administrador pode analisar todo o histórico de login do mesmo contendo a data, o ip de origem do dispositivo que utilizou a credencial do usuário e estado da autenticação.
m) O administrador pode gerar arquivos '.pcap' para quaisquer comunicação inspecionada pela solução.
n) O serviço deverá se integrar com serviço LDAP a fim de possibilitar a autenticação e autorização de usuários na interface de administração e para consultas com objetivos de enriquecer os dados inspecionados.
o) O serviço deverá permitir a utilização de segundo fator de autenticação para logins na interface web.
p) O serviço deverá possuir mecanismo de gerenciamento de usuários da interface web permitindo:
1. Criação, modificação ou remoção de usuários
2. Gerenciamento de permissionamento dos usuários.
3. Opção de gerar usuário com permissão de leitura apenas.
q) Deve possuir interface para visualização dos aspectos do sistema como:
1. A versão de software, espaço utilizado em disco, consumo de CPU e consumo de memória.
2. Informação de todas as interfaces ativas e respectivo tráfego recebido através de cada uma delas.
3. Total de banda processada no momento, a média de banda processada e o pico de banda registrado nas últimas semanas.
4. Uma análise detalhada de todo o tráfego recebido no dispositivo bem como a última vez em que os principais protocolos foram vistos dentre eles, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, dentre outros.
5. Listagem de todas as sub redes identificadas no ambiente bem como a quantidade de dispositivos em cada sub rede.
r) Deve permitir o envio de e-mails de alertas emitidos pela solução.
s) Deve permitir o envio de logs para sistemas externos utilizando os seguintes padrões:
1. CEF
2. LEEF
3. JSON
4. Syslog
5. Deve permitir a integração nativa com plataforma de gerenciamento de chamados como Atlassian JIRA e ServiceNow.
6. Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.
t) A plataforma deve possuir OPEN API para suportar integração com sistemas terceiros.
u) Deve possuir Inteligência artificial para automatizar triagens, análises e investigações de ameaças.
v) Deve possuir um aplicativo mobile capaz de visualizar, responder a incidentes, notificar, reportar e aprovar remediações para Android e iOS.
w) Deve possuir painel incorporado para executar consultas em metadados no tráfego inspecionado.

2.9.4. CARACTERÍSTICAS DE GERENCIAMENTO DE RELATÓRIOS

a) Deve permitir a criação automática de relatórios executivos cobrindo no mínimo:
1. Indicação da quantidade total de dispositivos, quantidade total de sub redes e banda média processada.
2. Sumário das violações por fase do ataque.

3. Sumário dos dispositivos com maior nível de brechas não usuais.
4. Sumário dos top dispositivos que mais violaram comportamentos anômalos.
5. Violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, dentre outros.
6. Sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.
7. Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv
b) Deve possuir mecanismo para busca de dados diretamente na base de dados da solução.
c) O administrador pode gerar pesquisas e relatório dos seguintes critérios, mas não limitados a:
1. Data e Horário
2. Endereços IPs de origem e destino
3. Versão do protocolo IP
4. Protocolo de comunicação
5. Estado da conexão
6. Dados trafegados de entrada e saída.
7. Método HTTP
8. Cabeçalhos HTTP
9. Versão do SSL
10. Cifragem da Conexão SSL
11. Logins Kerberos
12. Comunicações DNS
13. Comunicações FTP
14. Comunicações LDAP
15. Comunicações Kerberos
16. Comunicações de mineração de criptomoedas
17. Comunicações SMB
18. Comunicações Radius
19. Comunicações RDP
20. Comunicações SIP
d) A procura na base da solução deve apresentar resultados em menos de 5 minutos de execução independentemente do escopo da pesquisa.

2.9.5. REQUISITOS DE SERVIÇO

a) A Tecnologia deve permitir respostas autônomas, em segundos, capazes de responder a ataques mais modernos como ransomware (ex. Lockbit 3.0 Criptografa 100 mil arquivos em 4 minutos).
b) O Serviço de Gestão de Incidentes de Segurança deverá ser prestado em período integral (24x7 – vinte quatro horas por dia, sete dias por semana).
c) A qualquer momento o CONTRATANTE poderá solicitar, através de Requisição de Serviços, o atendimento presencial da CONTRATADA de qualquer dos serviços, para o tratamento de incidentes ou grave ameaça de segurança da informação.
d) As requisições de serviço serão solicitadas ordinariamente à CONTRATADA em reuniões mensais para serem executadas no mês subsequente a critério do CONTRATANTE, ou excepcionalmente, em caráter de urgência, através de e-mail.
e) A CONTRATADA deve realizar de forma proativa as ações necessárias para manter o ambiente de segurança da CONTRATANTE adequado às melhores práticas do mercado, devendo:
1. Atualizar os firmwares e/ou softwares das soluções entregues como parte do objeto deste Termo de Referência

(TR);
2. Propor os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes;
3. Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste TR, as mantendo documentadas e acessíveis no portal do cliente.
4. Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE;
f) A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todos as áreas de atuação do escopo do contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes;
g) A CONTRATADA deverá manter uma rotina mensal de análise de indicadores internos e pesquisa de mercado com o objetivo de apresentar à CONTRATANTE um relatório com as inovações tecnológicas e solução que possam aumentar a qualidade e o grau de maturidade da segurança da informação do ambiente tecnológico;
h) Monitorar permanentemente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;
i) Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
j) Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de Tecnologia da Informação e Comunicação (TIC) da CONTRATANTE;
k) Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;
l) Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
m) Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;
n) Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
o) Monitorar e propor soluções aos projetos/atividades em andamento, otimizando-os quanto aos requisitos de Segurança da Informação;
p) Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;
q) Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;
r) Para atendimento em específicos o SOC deve escalar para o time de elite do contratante, com intuito de realizar investigações mais especificas.

2.9.6. REQUISITOS COMUNICAÇÃO

a) Diariamente por e-mail deverá ser entregue um relatório em português sobre Comportamentos Anômalos encontrados, baseado no modelo do MItreAttack, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas;
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) A CONTRATADA deverá rever periodicamente as políticas e processos do SOC a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL 4;
e) A CONTRATADA deverá disponibilizar dashboards de acompanhamento em tempo real da operação do SOC

que permitam a validação dos indicadores acordados;
f) A CONTRATADA deverá apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;
g) A CONTRATADA deverá confeccionar relatórios técnicos pontuais sob demanda;
h) A CONTRATADA deverá disponibilizar acesso de leitura a todas as ferramentas utilizadas para a prestação do serviço, permitindo desta forma que a CONTRATANTE audite a correta entrega do objeto contratado;
i) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
j) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
k) É responsabilidade da CONTRATADA supervisionar as rotinas de backup e restauração dos equipamentos, softwares e configurações implantadas referentes a segurança da informação;
l) É responsabilidade da CONTRATADA supervisionar as rotinas periódicas configuradas referentes a segurança da informação;
m) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobre a criação ou atualizações de tiquetes.
n) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
o) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da contratada.
p) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.
q) Quando o SOC cria um Relatório de Incidente de Segurança, um ticket correspondente deve ser criado no portal e uma notificação por e-mail é enviada para a CONTRATANTE.
r) O CONTRATANTE deverá comunicar um ponto focal, responsável pelo nível de serviço.

2.9.7. REQUISITOS COMPATIBILIDADE E INTEGRAÇÕES

a) As Ferramentas a serem disponibilizadas pela CONTRATADA deverão ser compatíveis com o ambiente tecnológico da CONTRATANTE;
b) Cabe à CONTRATANTE fornecer infraestrutura necessária para a instalação das ferramentas que serão utilizadas na solução, exceto para a ferramenta de DEFESA CIBERNÉTICA.

2.9.8. REQUISITOS DA OPERAÇÃO DOS DISPOSITIVOS QUE COMPÕEM OS SERVIÇOS

a) A CONTRATADA deverá executar no prazo máximo de 90 (noventa) dias, a contar da data do memorando de início, as atividades de planejamento, instalação/adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, em conformidade com este Termo de Referência;
b) Todas as atividades e documentação apresentadas deverão ser previamente aprovados pela CONTRATANTE.
c) A CONTRATADA, como parte da execução do Serviço de Operação e Atendimento de Requisições, deverá realizar, nos primeiros 40 (quarenta) dias de execução deste serviço, uma avaliação completa do ambiente do contratante com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) e avaliar a maturidade dos controles de segurança da CONTRATANTE;
d) O GAP Analysis deverá ser realizado utilizando como base um dos seguintes frameworks de segurança: NIST, CIS ou ISO, que deverá ser antecipadamente aprovado pela CONTRATANTE;
e) A CONTRATADA, após o levantamento inicial das lacunas ou falhas de segurança da informação no ambiente da CONTRATANTE, deverá elaborar, coordenar e supervisionar um plano de ação em conjunto com a

CONTRATADA, priorizando as falhas consideradas mais críticas;
f) A CONTRATADA deverá seguir o processo de mudança estabelecido pela CONTRATANTE;
g) Todos os serviços previstos deverão ser implantados, documentados e revisados pela CONTRATADA, seguindo a metodologia ITIL 4;
h) A CONTRATADA, sempre que solicitada, deverá estar disponível para participar das reuniões internas com o CONTRATANTE, para prestar informações sobre os ambientes e serviços por elas executados;
i) Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas contratadas e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto;
j) A CONTRATADA deverá apresentar ao CONTRATANTE o planejamento ou plano de ação de todas as mudanças no ambiente, conforme níveis de controle estabelecidos, para todas as mudanças apresentadas;
k) A CONTRATADA deverá acompanhar, dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização;
l) A CONTRATADA deverá monitorar permanente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;
m) Todos os serviços de manutenção corretiva e preventiva são considerados de natureza continua e deverão minimizar a necessidade de parada do ambiente em produção;
n) Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais, conforme os requisitos específicos para o perfil profissional.

2.10. SERVIÇO DE INTELIGÊNCIA CIBERNÉTICA EM DARK E DEEP WEB

2.10.1. REQUISITOS DE NEGÓCIO

a) O Serviço de Inteligência Cibernética em Dark e Deep web deve se integrar ao SOC a ser entregue pela CONTRATADA no regime 24x7x365 para trazer uma visão holística do risco e ameaça.
b) O serviço de inteligência cibernética na Dark Web e Deep Web pode ajudar a CONTRATANTE a detectar proativamente ameaças cibernéticas antes que elas se tornem conhecidas ou causem danos significativos. Isso permite que a CONTRATANTE tome medidas preventivas para proteger seus ativos e dados.
c) O Serviço deve oferecer rastreamento da Dark Web e a Deep Web em busca de informações confidenciais ou dados da CONTRATANTE que possam ter sido roubados ou vazados. Dessa forma, a CONTRATANTE pode identificar rapidamente incidentes de violação e tomar medidas para mitigar os danos.
d) O Serviço deve ajudar a CONTRATANTE a identificar grupos de hackers e atores maliciosos que podem estar planejando ataques ou visando a organização. Com essa informação, a CONTRATANTE pode melhorar suas defesas e estar preparada para enfrentar possíveis ameaças.
e) Com o conhecimento adquirido na Dark Web e Deep Web, a CONTRATANTE pode tomar medidas proativas para evitar ataques futuros. Isso pode incluir o reforço de medidas de segurança e o treinamento de funcionários sobre práticas seguras na internet.

2.10.2. REQUISITOS TÉCNICOS E DE FUNCIONALIDADES PARA A REALIZAÇÃO DOS SERVIÇOS

a) O serviço deve realizar um monitoramento avançado e contínuo de fontes na Dark e Deep Web, buscando identificar ameaças e atividades maliciosas.
b) A equipe responsável pelo serviço deve ter conhecimento especializado e capacidade de acessar a Dark e Deep Web de forma segura e anônima.
c) O serviço deve coletar e analisar dados de forma automatizada e manual, buscando informações relevantes sobre ciberataques, grupos de hackers e atividades criminosas.

d) O serviço deve ser capaz de identificar ameaças emergentes, vazamentos de informações confidenciais, vulnerabilidades exploradas e ataques em planejamento.
e) Deve ser fornecida inteligência sobre novas táticas, técnicas e procedimentos utilizados por hackers e cibercriminosos na Dark e Deep Web.
f) O serviço deve analisar vulnerabilidades específicas que podem afetar a organização da CONTRATANTE e suas informações.
g) O serviço deve manter um índice atualizado de sites e fóruns da Dark Web para facilitar a busca e monitoramento de informações específicas.
h) A equipe do serviço deve realizar investigações proativas para identificar e rastrear ameaças que possam impactar a CONTRATANTE.
i) O serviço deve estar em conformidade com as regulamentações e leis aplicáveis ao monitoramento da Dark e Deep Web, garantindo a legalidade das atividades.
j) Todas as comunicações e compartilhamento de informações relacionadas ao serviço devem ser realizados de forma segura e criptografada.
k) A privacidade e anonimato dos clientes e dados da CONTRATANTE devem ser rigorosamente protegidos durante o monitoramento e análise.
l) O serviço deve fornecer relatórios detalhados sobre as ameaças identificadas, incluindo recomendações de mitigação e ações corretivas.
m) O serviço deve ser capaz de enviar alertas em tempo real sobre ameaças iminentes ou atividades suspeitas encontradas na Dark e Deep Web.
n) O serviço pode realizar testes de simulação de ameaças para avaliar a eficácia das defesas da organização da CONTRATANTE.
o) O serviço deve se manter atualizado com as tendências e evoluções da Dark e Deep Web, aprimorando continuamente suas técnicas de coleta e análise de dados.
p) O serviço deve ser capaz de gerenciar incidentes relacionados à Dark e Deep Web, conduzindo investigações, coleta de evidências e relatórios apropriados.
q) O serviço de "Inteligência Cibernética em Dark e Deep Web" é subdividido em 2 componentes:
1. Serviço de Coleta;
2. Serviço de Processamento de Dados e Apresentação.
r) O Serviço de Coleta de vulnerabilidades e dados estratégicos se dá a partir de fontes estruturadas e não estruturadas existentes na rede mundial de computadores. Ele é pautado em uma ontologia aderente às finalidades de Segurança da Informação e Proteção de Dados, sem restringir-se à mera busca literal de palavras-chave, de modo a explorar semanticamente todas as possibilidades que os canais monitorados oferecem. O serviço ainda conta com um sistema de notificação automática das vulnerabilidades coletadas, de forma que o analista possa tratar a informação com oportunidade.
s) Para tanto, o Serviço de Coleta é dividido de acordo com seu escopo, sendo composto pelas seguintes categorias:
1. Coleta Direta no Escopo;
2. Coleta por Simulação;
3. Coleta por Vulnerabilidade;
4. Coleta por Reporte Estruturado;
5. Coleta por Reporte Difuso; e
6. Coleta de Dados Estratégicos.
t) O Sistema de Processamento de Dados e Apresentação representa o software responsável por armazenar e processar os dados obtidos pelo Serviço de Coleta, bem como apresentar as informações ao analista. Seu objetivo

é incrementar a capacidade de processamento analítico do Espaço Cibernético de Interesse (ECI), de modo a permitir o acesso, a visualização e a análise dos dados com alta flexibilidade e performance, em diferentes dimensões ou perspectivas, bem como a identificação de padrões e tendências no universo amostral coletado; além da detecção preditiva das ameaças provenientes da dimensão cibernética.

u) Para tal, o Sistema de Processamento de Dados e Apresentação deve representar as informações em modo gráfico e sintético para que a autoridade assessorada possa decidir sobre as ações factiveis ao longo de um prazo de tempo diante de um contexto específico. Isto se dá por meio de:

1. uma interface gráfica com menus e links intuitivos;
2. relatórios personalizáveis;
3. mapas georreferenciados;
4. diagramas de vínculos;
5. linhas temporais;
6. envio de notificações;
7. envio de alertas;
8. exportação e importação de dados em formatos padronizados.

v) Capacidade de realizar cada uma das categorias de coleta que compõem o Serviço de Coleta;

1. Utilizar técnicas de Big Data e de mineração de dados (data mining) no tratamento e análise dos dados;
2. Permitir consultas em estruturas de pesquisa estática e dinâmica;
3. Requisitos de Segurança da Solução;
4. Requisitos de Interface do Usuário.

w) A Coleta no Escopo Direto é aquela na qual os incidentes relativos aos sistemas e serviços acessíveis por meio da Internet, que incidam sobre o Escopo Interno, são coletados de forma convencional e sem o emprego de técnicas invasivas.

x) No caso de a Coleta no Escopo Direto sobrecarregar os ativos analisados, sua frequência será ajustada junto à CONTRATANTE.

y) No caso de qualquer dano à plena funcionalidade dos elementos analisados, a CONTRATADA deverá tempestiva e imediatamente interromper os procedimentos de coleta e ajustar, junto à CONTRATANTE, seus parâmetros.

z) A Coleta no Escopo Direto deve abranger, pelo menos, as categorias abaixo especificadas:

1. Desfiguração de sítio:

I. Identificação de páginas com conteúdo incompatível com o original, fruto de ações de pichação ou manifesto político-ideológico publicado inadvertidamente por invasores.

II. As coletas devem ser realizadas somente nas páginas principais de cada aplicação web.

III. A desfiguração deve ser identificada, no mínimo, a partir da análise do código-fonte estático da página ou da identificação de palavras nas imagens do sítio e a partir de mecanismos de OCR (Optical Character Recognition), segundo palavras-chave constantes de um dicionário, a ser fornecido pela CONTRATANTE, relacionado à ontologia em pauta.

2. Indisponibilidade de domínios

I. Assinalação de sítios indisponíveis a partir da Internet.

II. A ocorrência será considerada a partir de 5 (cinco) minutos de indisponibilidade comprovada.

III. Uma notificação também deverá ser enviada quando o sítio retornar à situação de disponibilidade, incluindo o período total de indisponibilidade.

3. Diretórios sensíveis:

I. Assinalação de diretórios com conteúdo sensível ou áreas administrativas acessíveis livre e indiscriminadamente a terceiros.

II. A coleta de Diretórios Sensíveis deve ser realizada, no mínimo, nos caminhos especificados em dicionário a ser fornecido pela CONTRATANTE, considerados a partir da raiz da página principal.
4. Exposição de dados:
I. Assinalação de dados expostos em arquivos disponíveis inadvertidamente em aplicações web voltadas para a Internet.
II. As coletas devem ser realizadas, no mínimo, nos arquivos especificados no dicionário a ser fornecido pela CONTRATANTE, considerados a partir da raiz de cada sítio do Escopo Interno.
aa) As ocorrências coletadas que preencham os requisitos de relevância acima descritos devem ser persistidos com os seguintes dados:
1. URL da ocorrência;
2. Timestamp da detecção da ocorrência;
3. Categoria do incidente; e
4. Código fonte da página assinalada, nos casos de Desfiguração de Sítios e de Exposição de Dados, de modo que se a postagem original venha a ser removida pelo seu autor ou por terceiros, o conteúdo do registro seja ainda acessível.
bb) No caso de O serviço proposto abranger outras categorias de Coleta no Escopo Direto, o serviço deverá ser previamente analisado pela CONTRATANTE, a fim de verificar impactos no Escopo Interno.

2.10.3. COLETA POR SIMULAÇÃO

a) A Coleta por Simulação consiste no registro de incidentes a partir de ambientes virtuais simulados ou emulados (honeynets e honeypots), a fim de detectar ações de varreduras e ataques e que sejam relacionados às redes do Escopo Interno.
b) Quantidade e geolocalização mínima dos servidores honeypot:
1. 3 (três) no Brasil, em qualquer região da federação;
2. 1 (um) na América do Sul, em qualquer país, exceto Brasil;
3. 1 (um) na América Central, em qualquer país do continente;
4. 1 (um) na América do Norte, em qualquer país do continente;
5. 1 (um) na Europa, em qualquer país do continente;
6. 1 (um) na Ásia, em qualquer país do continente; e
7. 1 (um) na Oceania, em qualquer país do continente.
c) Esta categoria de coleta deve ter a capacidade de identificar e armazenar, sempre que disponível, as seguintes informações:
1. Endereço IP e porta associada à origem potencialmente maliciosa;
2. Domínio reverso associado ao endereço IP da ocorrência;
3. Geolocalização do endereço IP da origem potencialmente maliciosa;
4. Payload de resposta obtido por meio da requisição formulada como teste da Vulnerabilidade notória ou ponto de exploração;
5. Login e senha em caso de tentativa de autenticação no honeypot; e
6. Exemplares dos malwares obtidos.

2.10.4. COLETA DE VULNERABILIDADES

a) A Coleta de Vulnerabilidades consiste na detecção de vulnerabilidades conhecidas ou de pontos de exploração em aplicações e redes contempladas no Escopo Interno.
b) A Coleta de Vulnerabilidades deverá utilizar, no mínimo, os serviços Shodan, Censys e ZoomEye.
c) Esta categoria deve contemplar, ao menos, as seguintes ocorrências:

1. Serviços dos protocolos RDP, FTP, VNC e Telnet cujo acesso possa ocorrer remotamente e permita ao atacante acesso à área administrativa do servidor-alvo em função de acesso sem a autenticação do usuário ou com autenticação anônima.
2. Servidores dos protocolos DNS e NTP suscetíveis a amplificação de ataques de negação de serviço (Denialof Service – DoS), transferência de zona ou configurados de forma a resolver domínios maliciosamente, conduzindo o usuário a páginas falsas.
3. Bancos de dados ou storages PostgreSQL, MySQL, SQLServer, Oracle e Elastic Search, MongoDB, Iomega cujo acesso possa ocorrer remotamente sem a presença de autenticação ou que permitam ataque de força bruta para o acesso indevido.
4. Certificados SSL expirados ou inválidos e sistemas que não utilizem HTTPS.
5. Sistemas suscetíveis, no mínimo, aos ataques HeartBleed, Freak, Poodle, BEAST e Logjam.
6. Serviços FTP, NetBIOS, SMB, SSH e VPN cuja configuração equivocada possa permitir o mapeamento de ativos em redes não públicas e identificação de serviços acessíveis remotamente.
7. Equipamentos e artefatos classificados como Internet das Coisas (Internet ofThings – IoT) acessíveis remotamente por meio da Internet, dentre os quais, os dispositivos de rede, as impressoras e as câmeras de monitoramento.
d) Esta categoria deve ter a capacidade de identificar e armazenar, sempre que disponíveis, as seguintes informações:
1. Vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração;
2. Timestamp da detecção da ocorrência;
3. Endereço IP e porta associada à vulnerabilidade ou ponto de exploração;
4. Domínio reverso associado ao endereço IP da ocorrência;
5. Geolocalização do endereço IP onde a URL da ocorrência está hospedada;
6. Identificação do provedor de conexão (ISP) do endereço IP;
7. Payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração;
8. Resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste;
9. As classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE);
10. Os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web;
11. O cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS;
12. A relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.
e) A lista de Google Dorks deverá ser utilizada pela solução para executar uma nova coleta, por meio de varreduras referentes aos sítios do Escopo Interno, em período a ser definido junto à CONTRATANTE, devendo retornar a relação de sistemas web vulneráveis, sem, no entanto, realizar o teste invasivo da suposta vulnerabilidade.

2.10.5. COLETA POR REPORTE ESTRUTURADO

a) A Coleta por Reporte Estruturado representa a coleta de incidentes sobre o Escopo Interno a partir de fontes que apresentam os dados de forma concentrada e estruturada.
b) A Coleta por Reporte Estruturado deve incidir, no mínimo, sobre os seguintes serviços:
1. Compartilhamento de desfigurações nos portais: Zone-H, Defacer ID e Mirror-H.
2. Divulgação de vulnerabilidades nas plataformas de bug bounty: Open Bug Bounty e BugHeist.

3. Blacklists: AbuseIPDB, UCEProtect, OpenCTI.br, NUBI e MalwareWorld.
4. Compartilhamento de phishing: Phishtank e Openphish.
5. Compartilhamento de malware: VirusTotal, HybridAnalysis e ANY.RUN.
6. Compartilhamento de arquivos na rede BitTorrent.
c) Os registros coletados nos serviços acima devem manter a persistência dos seguintes dados:
1. URL da ocorrência;
2. Finalidade do domínio no contexto coletado (distribuição, comando e controle, redirecionamento para atividade maliciosa ou outra classificação plausível);
3. Timestamp da detecção do incidente;
4. Entidade alvo da atividade maliciosa, no caso de phishing (a página ou serviço de quem se pretendia simular);
5. Artefato malicioso identificado como provocador no caso do phishing;
6. Detalhes sobre a autoria do incidente (no caso de desfiguração, o grupo ao qual se atribui o ataque, bem como seu indivíduo notificador);
7. Características da máquina atacada (sistema operacional, servidor web e a forma de ataque declarada);
8. Registros em espera de validação (onhold), no caso de incidentes de desfiguração, sendo que o processo de coleta deve incluir a validação automatizada das desfigurações, realizando uma Coleta no Escopo Direto, de modo a impedir a persistência de falsos positivos desse tipo de incidente;
9. Evidência do ocorrido, no caso de incidentes de desfigurações, consubstanciada na forma de printscreen e de obtenção do código HTML fonte da página afetada;
10. Evidência e indicação do domínio do Escopo Interno afetado, no caso de malwares.

2.10.6. COLETA POR REPORTE DIFUSO

a) A Coleta por Reporte Difuso representa a coleta de incidentes sobre o Escopo Interno a partir de fontes em que apresentam os dados dispersos e de forma não estruturada.
b) A Coleta por Reporte Difuso deve incidir, no mínimo, sobre os seguintes serviços ou canais de comunicação:
1. As redes sociais Twitter e Reddit;
2. O serviço de compartilhamento de vídeos YouTube;
3. Os serviços de compartilhamento de texto Pastebin.com e Ghostbin.com;
4. Os serviços de compartilhamento de código GitHub e GitHub Gist;
5. Os canais de comunicação IRC, Telegram e DiscordApp, Slack,Mattermost e Rocket.Chat;
6. Fóruns hacker na surface e na dark web; e
7. Os endereços .onion, a serem definidos junto à CONTRATANTE e/ou previamente mapeados pela CONTRATADA.
c) Quando necessário, a CONTRATANTE fornecerá o convite de acesso aos serviços e canais de comunicação mencionados acima.
d) São considerados temas de interesse para Coleta por Reporte Difuso, as publicações que versarem sobre a incitação, a ameaça ou o relato de ataque cibernético a ativos do Escopo Interno nas seguintes modalidades:
1. Negação de serviço (Deny of Service - DoS);
2. Desfiguração de página (defacement), pautado pela ontologia disposta em dicionário a ser fornecido pela CONTRATANTE;
3. Vazamento de dados, incluindo bases de dados (dumps), credenciais de acesso (leaks), exposições de dados pessoais (exposed);
4. Exposições de configurações sensíveis de aplicações ou de seus respectivos códigos fonte;
5. Exposições de dados sensíveis, de acordo com a ontologia pautada em palavras-chave provenientes de um dicionário a ser fornecido pela CONTRATANTE;

6. Invasão de sistema ou equipamento;
7. Phishing;
8. Ransomware;
9. Ferramentas e exploits.

e) Os registros que preencham os temas acima descritos devem ser coletados, sempre que possível e obedecendo as características de cada serviço ou canal de comunicação, com a persistências dos seguintes dados:

1. URL da ocorrência;
2. Timestamp da detecção da ocorrência;
3. Código fonte da postagem ou o conteúdo relevante assinalado, de modo que se a postagem original venha a ser removida pelo seu autor ou por terceiros, o conteúdo do registro seja ainda acessível;
4. Domínios e URL mencionadas (incluídas credenciais de acesso com base em endereços de correio eletrônico) que estiverem associadas ao escopo de incidência da coleta;
5. Mídias anexadas ao texto da postagem (imagens e vídeos) em qualquer um dos canais monitorados;
6. Dados disponíveis sobre o autor/canal da publicação, tais como a imagem/avatar, o texto descritivo do perfil ou canal, a localidade declarada do perfil ou canal, o número de seguidores ou amigos, o número de perfis que o autor segue e a quantidade total de publicações (aplicável às coletas de incidentes sobre redes sociais e canais de compartilhamento de vídeos e dos canais de comunicação);
7. Endereço IP indicado como alvo da ferramenta/exploit;
8. Domínio indicado como alvo da ferramenta/exploit; e
9. Classificação de CVE que foi atribuída à ferramenta/exploit.

2.10.7. COLETA DE DADOS ESTRATÉGICOS

a) A Coleta de Dados Estratégicos consiste na coleta de dados públicos relativos às características cibernéticas de Estados, nações e Ameaças Avançadas Persistentes (AdvancedPersistentThreats – APT), que incidam sobre o Escopo Externo, a fim de fornecer uma visão global do ECI a elementos decisores.

b) Em relação às APT, devem ser utilizados relatórios públicos sobre essas ameaças, e quando disponíveis, devem ser coletados e armazenados, no mínimo, os seguintes dados:

1. Grupo ou país ao qual se atribuiu a APT;
2. Se há menção a patrocínio ou suporte estatal;
3. Países alvos do ataque;
4. Os indicadores de comprometimento que tenham sido disponibilizados (endereços IP, domínios, hashes e nomes de arquivos);
5. As CVE (Common Vulnerabilities and Exposures) que tenham sido empregadas na realização do ataque descrito;
6. As principais técnicas, táticas e procedimentos que tenham sido utilizadas para realização da ação;
7. Backdoors empregados na realização do ataque;
8. Amostras dos artefatos empregados na realização do ataque; e
9. O período indicado de atividade da APT.

2.10.8. CONSULTAS EM ESTRUTURAS DE PESQUISA ESTÁTICAS

a) As Consultas em Estruturas de Pesquisa Estáticas são perguntas previamente definidas pela CONTRATADA frente a cenários de interesse específico da mesma. Por exemplo, buscar determinada vulnerabilidade, ou determinado atacante.

b) As consultas em cada cenário especificado devem ser apresentadas de forma gráfica e transparente.

c) Cada consulta, quando pertinente, deve disponibilizar o histórico de eventos relacionados, de modo a

correlacionar as ocorrências sob a dimensão temporal.
d) As informações devem ser apresentadas, no mínimo, segundo os seguintes cenários de interesse:
1. Domínio;
2. Categoria de Incidente;
3. Atacante;
4. Vulnerabilidade;
5. País;
6. APT;
7. Simulação.
e) Estes cenários devem agrupar os elementos pertinentes e apresentar links para outros, quando cabível.
f) Exemplo do fluxo de análise:
1. Operador acessa a relação dos domínios de terceiro nível no Escopo Interno com o maior número de desfigurações no mês.
2. Por meio de hiperlink, o operador acessa o primeiro domínio da lista, acessando o cenário daquele domínio, que inclui o histórico de ataques sofridos, bem como a listagem dos atacantes relacionados.
3. Clicando no elemento responsável pelo maior número de ataques, o analista é levado ao seu cenário, que inclui o diagrama de vínculos e o histórico de ataques, o qual é filtrado para exibir os ataques da última semana.
4. A partir da análise realizada, o operador é capaz de identificar que aquela entidade apresentou alto índice de desfigurações em um segmento específico do Escopo, todas utilizando a mesma técnica.
5. O analista exporta as evidências pertinentes e age preventivamente, alertando outros segmentos da organização que possam vir a se tornarem alvos.
g) Requisitos de Consulta dos Cenários de Interesse:
1. Cenário de Domínio
I. Relação de incidentes detectados, agrupados por categoria e por evento.
II. Relação de atacantes com alvo no domínio.
III. Relação de eventos de indisponibilidade de sítio, contendo duração aproximada.
2. Cenário de Categoria de Incidente:
I. Desfiguração de Sítio
II. Indisponibilidade de Domínio;
III. Diretórios Sensíveis;
IV. Exposição de Dados; e
V. Inclusão em Blacklist.
3. Para cada categoria de incidente, quando houver a caracterização de um ataque, apresentar relação de:
I. Atacantes, classificados de acordo com os graus de atividade (frequência de Ataques somados à frequência de posts em mídias sociais);
II. Domínios e subdomínios com maior quantidade de ataques, total e por categoria.
4. Categoria de Incidente Desfiguração de Sítio.
I. Relação dos principais incidentes de desfiguração, ordenados de acordo com a quantidade de incidentes detectados.
5. Categoria de Incidente Indisponibilidade de Domínio
I. Realizar o cálculo aproximado de disponibilidade (uptime) e indisponibilidade (downtime) do domínio.
II. Relação de domínios com maior indisponibilidade, a partir do intervalo temporal selecionado pelo usuário, ordenando por casos de indisponibilidade com maior duração para cada domínio.
III. Contabilizar a frequência de sucessos e de falhas na verificação de disponibilidade dos domínios.
6. Categoria de Incidente Diretórios sensíveis

I. Relação dos principais diretórios sensíveis expostos, ordenados de acordo com a quantidade de incidentes detectados.
II. Relação dos serviços com diretórios expostos.
7. Categoria de Incidente Exposição de Dados
I. Relação dos principais tipos de dados expostos, ordenados de acordo com a quantidade de incidentes detectados.
8. Categoria de Incidente Inclusão em Blacklist
I. Relação de domínios ou AS do Escopo Interno em blacklist.
9. Cenário de Atacante
I. Correlacionamentos dos perfis de ameaças agindo em grupos ou individualmente, monitorando suas atividades entre plataformas distintas.
II. Diagrama de vínculos entre atacantes, explicitando a relação entre diversas entidades, singulares ou coletivas.
10. Cenário de Vulnerabilidade
I. Relação de sítios vulneráveis, classificados por severidade e frequência.
II. Relação de vulnerabilidades do Escopo Interno, classificadas por severidade e frequência.
III. Totais de vulnerabilidades por tipo e categoria de vulnerabilidade e a respectiva avaliação de risco, seguindo as metodologias do MITRE (CVE) e do NIST.
IV. Possibilidade de integração de consultas com bases de exploits (ao menos Exploitdb.com).
11. Cenário de País
I. Mapa-múndi interativo, georreferenciado, no qual seja possível selecionar um país e obter seu perfil cibernético, sendo apresentados todos os dados coletados das fontes previamente definidas.
II. Para cada perfil cibernético de país, disponibilizar a relação de APTs a que se atribui patrocínio estatal, contendo links para os relativos cenários.
12. Cenário de APT
I. Relação de principais APTs, com links para os perfis de cada grupo.
II. Para cada perfil de APT, disponibilizar relatórios, links e demais fontes públicas relativas à ameaça;
III. Denominações diversas da ameaça;
IV. Descrição sucinta e informativa da ameaça;
V. Principais operações e alvos, contendo descrição sucinta sobre os ocorridos;
VI. Para cada operação, apresentar fontes que versem sobre o tema;
VII. País de atribuição;
VIII. Principais ferramentas e malwares utilizados pela ameaça;
IX. Tabela MITRE ATT&CK™ com principais TTPs utilizadas;
X. Indicadores de Comprometimentos (IoC) referentes a possíveis ações da ameaça (assinaturas de vírus e endereçamento IP, hashes MD5 do malware ou URL ou nome do domínio dos servidores da botnet de comando e controle); e
XI. As CVE (Common Vulnerabilities and Exposures) que tenham sido exploradas na realização do ataque descrito.
XII. Possibilidade de análise das APTs sob outras dimensões, tais como: país, período de tempo ou TTP.
13. Cenário de Simulação
I. Principais combinações de usuários e senhas em cada serviço e nototal.
II. Origens dos ataques.
III. Linha temporal de ataques.
IV. Análise dos ataques sob diferentes dimensões, como por IP, país, AS, protocolo e porta.

2.10.9. CONSULTAS EM ESTRUTURAS DE PESQUISA DINÂMICAS

a) As Consultas em Estruturas de Pesquisa Dinâmicas são perguntas ad-hoc que devem ser respondidas por meio da manipulação e análise de um grande volume de dados sob múltiplas perspectivas.
b) O serviço deve ser capaz de:
1. Realizar busca textual com base em filtro de texto completo (full-textsearch) sobre todos os tipos de registros e todos os campos de conteúdo e de características gerais. A busca em texto completo deve, ainda, permitir a indicação de campo de conteúdo específico, por exemplo: autor, domínio, titulo.
2. Realizar busca de registros com base em filtro de expressões regulares (regular expression ou regex) de modo a permitir a busca por padrão de texto sobre todos os tipos de registros e todos os campos de conteúdo e de características gerais.
3. Realizar busca com base em filtro na origem do dado (fontes onde as coletas foram realizadas).
4. Realizar busca com base em filtro no tipo do dado (por exemplo: vulnerabilidades identificadas, phishings, ransomware, etc).
5. Realizar busca com base em filtro nas datas dos incidentes, sendo possível a fixação de intervalos para pesquisa (intervalo mensurado entre horas e anos).
6. Realizar buscas de acordo com características gerais (por exemplo: endereço IP, domínio registado) ou específicas (por exemplo: o status do registro de phishing) das ocorrências.
7. Realizar buscas com base em lapso temporal.
8. Combinar múltiplos filtros sucessivos que devem contemplar todos os campos dos registros.
9. Realizar a contagem de termos de quaisquer dos tipos de registro contidos na base de dados de coletas (por exemplo: nome de atacante, domínio, ISP).

2.10.10. EXPORTAÇÃO E IMPORTAÇÃO DE DADOS

a) O serviço deverá efetuar a emissão de relatórios customizáveis com base tanto nas Consultas em Estruturas de Pesquisa Estáticas quanto nas Dinâmicas, priorizando-se recursos gráficos que permitam maior velocidade na obtenção da consciência situacional;
b) O serviço deverá efetuar a elaboração de gráficos de diversos tipos que respondam dinamicamente à combinação de múltiplos filtros, simultâneos ou sucessivos, e que sejam exportados junto aos dados brutos selecionados;
c) O serviço deverá efetuar a elaboração de tabelas dinâmicas, que permitam a inclusão ou remoção de colunas na exportação dos dados ou geração de gráficos;
d) O serviço deverá efetuar a exportação dos dados de uma consulta, no mínimo, nos formatos CSV, XML e JSON; e 4.3.5. a importação dos dados, no mínimo, nos formatos CSV, XML e JSON.

2.10.11. REQUISITOS DE SERVIÇO

a) O serviço deve oferecer monitoramento contínuo de um número específico de domínios específicos da CONTRATANTE presentes na Dark e Deep Web.
b) O serviço deve incluir monitoramento especializado de atividades cibernéticas relacionadas a indivíduos ou grupos específicos considerados VIPs pela CONTRATANTE.
c) O serviço deve fornecer a capacidade de realizar takedowns (remoção) de conteúdo malicioso ou prejudicial encontrado na Dark e Deep Web que possa afetar a CONTRATANTE.
d) O serviço deve coletar e analisar dados relevantes relacionados aos domínios específicos, VIPs e atividades identificadas na Dark e Deep Web.
e) Devem ser fornecidos relatórios customizados que destaquem os insights mais relevantes relacionados aos domínios, VIPs e atividades monitoradas.
f) O serviço deve utilizar técnicas de inteligência avançadas para correlacionar dados e identificar padrões que

possam ser relevantes para a CONTRATANTE.
g) A CONTRATADA deve contar com ferramentas especializadas e recursos de automação para otimizar a eficiência do serviço.
h) A equipe do serviço deve garantir a proteção da identidade da CONTRATANTE e a confidencialidade dos dados durante a realização das atividades de inteligência cibernética.
i) O serviço deve estar disponível para suporte e atendimento de emergências 24 horas por dia, 7 dias por semana, devido à natureza continua das ameaças cibernéticas.
j) O serviço deve fornecer atualizações em tempo real sobre atividades relevantes, garantindo a agilidade na resposta a possíveis riscos.
k) Deve ser fornecido relatório detalhado sobre as ações de takedown realizadas, com informações sobre o conteúdo removido e as medidas adotadas.
l) A CONTRATADA deve operar em conformidade com a legislação aplicável para atividades relacionadas à Dark e Deep Web, garantindo a legalidade das ações.
m) Deve ser firmado um acordo de confidencialidade entre a CONTRATADA e a CONTRATANTE para proteger informações sensíveis e os detalhes do serviço prestado.

2.10.12. REQUISITOS DE COMUNICAÇÃO

a) Sempre que solicitado pela CONTRATANTE a CONTRATADA deverá por e-mail ou outro meio estabelecido previamente, deverá ser entregue um relatório em português sobre status do serviço, com métricas e sugestões de melhoria, com comentários do especialista.
b) Deverá haver ao menos 01 (uma) reunião mensal para apresentação dos resultados dos serviços prestados, de acordo com a disponibilidade da CONTRATANTE, caso seja necessário outras reuniões poderão ser solicitadas;
c) A CONTRATADA deverá realizar quadrimestralmente a pesquisa de qualidade operacional, documentando e disponibilizando os resultados para a contratante em reunião presencial, podendo essa periodicidade ser redefinida em comum acordo com a CONTRATANTE;
d) É responsabilidade da CONTRATADA supervisionar os procedimentos para abertura e atendimento a chamados referentes a segurança da informação;
e) É responsabilidade da CONTRATADA supervisionar os procedimentos de recuperação de equipamentos referentes a segurança da informação;
f) É responsabilidade da CONTRATADA supervisionar as rotinas de backup e restauração dos equipamentos, softwares e configurações implantadas referentes a segurança da informação;
g) Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a CONTRATANTE sobre a criação ou atualizações de tiquetes.
h) A CONTRATANTE pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.
i) Ao trocar informações sensíveis, estas devem utilizar a plataforma de comunicação segura da contratada.
j) A CONTRATANTE poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.
k) Quando o SOC cria um Relatório de Incidente de Segurança, um ticket correspondente deve ser criado no portal e uma notificação por e-mail é enviada para a CONTRATANTE.
l) O CONTRATANTE deverá comunicar um ponto focal, responsável pelo nível de serviço.

2.10.13. REQUISITOS DE COMPATIBILIDADE E INTEGRAÇÕES

a) O serviço deve ser compatível com diversas fontes de dados presentes na Dark e Deep Web, incluindo sites, fóruns, blogs, redes sociais e outras plataformas de comunicação.
b) Deve ser capaz de interagir com diferentes protocolos de comunicação utilizados na Dark e Deep Web, como o protocolo TOR, I2P e outros protocolos anônimos.
c) O serviço deve ser integrável com ferramentas de coleta e análise de dados específicas para monitorar e extrair informações relevantes da Dark e Deep Web.
d) Deve fornecer APIs e web services bem documentados para facilitar a integração com sistemas e aplicações existentes da CONTRATANTE, como SIEM (Security Informationand Event Management) e outras soluções de segurança.
e) Deve ser compativel com sistemas de gerenciamento de incidentes utilizados pela CONTRATANTE, facilitando o registro e acompanhamento de incidentes de segurança cibernética.
f) O serviço deve ser compativel com diferentes tipos de bancos de dados para armazenar e gerenciar informações coletadas da Dark e Deep Web.
g) Deve ser capaz de integrar-se a soluções de análise de Big Data para processar e analisar grandes volumes de informações coletadas na Dark e Deep Web.
h) O serviço deve ser integrável com sistemas de automação de segurança utilizados pela CONTRATANTE para facilitar a resposta rápida a ameaças.
i) O serviço deve estar em conformidade com os padrões de segurança e criptografia necessários para garantir a proteção adequada das informações coletadas e armazenadas.
j) Deve garantir que a comunicação entre o serviço e outros sistemas seja criptografada e protegida contra ameaças de interceptação.
k) Deve ser compativel com aplicativos e sistemas móveis para permitir o acesso e o monitoramento em dispositivos móveis da CONTRATANTE.
l) O serviço deve ser capaz de integrar-se com fontes externas de inteligência de ameaças para enriquecer as informações coletadas e ampliar a capacidade de detecção de ameaças.
m) Deve ser atualizado regularmente para se adaptar às mudanças nas tecnologias, protocolos e fontes de dados da Dark e Deep Web.

2.10.14. REQUISITOS DE OPERAÇÃO DOS SERVIÇOS

a) É necessário configurar uma rede segura e isolada para o serviço, garantindo a proteção dos dados e a prevenção de vazamentos de informações sensíveis.
b) Deve ser configurada uma VPN (Virtual Private Network) e proxies para garantir a navegação segura e anônima na Dark e Deep Web.
c) Devem ser aplicadas técnicas de criptografia para proteger os dados coletados e armazenados pelo serviço.
d) Devem ser estabelecidos controles de acesso adequados, garantindo que apenas pessoal autorizado possa acessar o serviço e as informações sensíveis.
e) É necessário realizar testes de segurança e penetração para identificar possíveis vulnerabilidades no sistema e garantir a sua proteção contra ataques.
f) Deve ser realizada uma revisão das políticas de segurança para garantir que estejam em conformidade com as melhores práticas e regulamentações aplicáveis.

2.11. SERVIÇO DE CONSULTORIA DE CIBERSEGURANÇA EM SUPORTE ESPECIALIZADO

2.11.1. REQUISITOS DE NEGÓCIO

a) A CONTRATANTE busca serviços de consultoria em segurança da informação, para trazer maior proteção aos colaboradores, bem como os clientes atendidos pela CONTRATANTE.

b) Devem ser utilizadas as ferramentas de segurança da CONTRATADA e da CONTRATANTE para realização do serviço de consultoria.
c) Os serviços poderão ser executados de forma remota, a partir das localidades de trabalho do SOC (Centro de Operações de Segurança) e Serviço Gerenciado de Segurança da CONTRATADA.
d) Estes serviços deverão ser executados em modelo 8x5xNBD.
e) Entende-se por horário de atendimento 8x5xNBD de segunda a sexta, a partir das 08:00 até às 17:00.
f) A contratante fornecerá todas as informações necessárias para execução do serviço e tomada de decisão sobre um determinado item, tentando, ao máximo, seguir a recomendação e expertise da CONTRATADA.
g) Conforme definição da CONTRATANTE, a CONTRATADA deverá ser responsável pelo Serviço de Consultoria para Melhoria Operacional da Segurança da Informação e apoio com ações evolutivas, no modelo de banco de horas.

2.11.2. QUANTITATIVOS

a) A CONTRATANTE estimou os seguintes quantitativos de serviços entregues para CONTRATADA para atender às necessidades da CONTRATANTE.
b) Para a prestação de serviço deverá prever 1 recurso como gestor da qualidade das entregas da operação para coordenar o alinhamento com a CONTRATANTE conforme a necessidade para ajustar os entregáveis.
c) A CONTRATADA deverá disponibilizar, para realização dos serviços, pelo menos 15 profissionais sênior por ½ período diário ou equivalente, que não extrapole o limite de horas apresentado abaixo:

2.11.3. CARACTERÍSTICAS GERAIS DO SERVIÇO DE CONSULTORIA

a) Esse serviço estará integrado com um conjunto de ferramentas, processos e equipe, no qual todas as ações de segurança serão centralizadas e dentro de um fluxo contínuo e correlacionado, de forma uniforme para a segurança esperada, sendo responsável por garantir que possíveis incidentes sejam corretamente identificados, analisados, defendidos, investigados e relatados.
b) O serviço deverá contemplar uma solução para varredura de vulnerabilidades, testes de intrusão, “phishing” testes como serviço – SaaS, Implantação, Manutenção, Relatórios e Treinamentos
c) A solução de análise de vulnerabilidades à ser adotada, as varreduras de vulnerabilidades do ambiente, os testes de intrusão, os testes de “phishing” e geração dos relatórios técnicos e executivos, deverão proporcionar visibilidade e informações sobre como está a segurança de todo ambiente computacional da CONTRATANTE, possibilitando assim uma melhoria continuada do ambiente computacional, adotando boas práticas de segurança e aplicação das correções necessárias, garantindo assim um ambiente com maior segurança e consciência do que precisa ser melhorado padronizado.
d) Deverá ainda normatizar as melhores práticas para aumentar a segurança (Hardening) de Endpoints e Aplicativos para ameaças virtuais à CONTRATANTE.
e) Deve abranger a execução, participar e apoiar projetos e iniciativas de melhoria operacional da Segurança da Informação, tais como Consolidações, atualizações tecnológicas, migrações, integrações e desativações.
f) Deve planejar ações de melhoria, propor soluções, acompanhar a sua implementação, e apoiar a verificação da eficácia dos resultados de acordo com as orientações e padrões da Segurança da Informação da CONTRATANTE ou por delegação pelas gerências de TI.
g) Deve elaborar e atualizar documentações e procedimentos necessários para administração, operação e suporte do ambiente gerenciado, garantindo sua atualização sempre que necessário.
h) Deve esclarecer dúvidas, fornecer informações e/ou orientações técnicas, necessárias para O serviço de problemas detectados no ambiente gerenciado.
i) Deve operacionalizar e acompanhar controles e requisitos de segurança da informação para ativos de TIC

definindo sua conformidade conforme orientações e recomendações da Segurança da Informação da CONTRATANTE;

j) Deve ser capaz de demonstrar capacidade de responder a ataques ransomware com sucesso de recuperação, diante da crescente ameaça representada por ataques ransomware, desenvolvendo e implementando estratégias de resposta que visam não apenas conter a propagação do ataque, mas também restaurar operações normais de maneira eficaz e eficiente, com abordagem de análise forense avançada e tecnologias capaz de mitigar os danos causados por esses ataques.

k) Deve operacionalizar o processo de acompanhamento de eventos emergenciais de segurança da informação na TI, validando sua eficácia e evolução através de itens de controle mensuráveis;

l) A CONTRATADA, sob demanda da CONTRATANTE, deve apresentar relatório de inconformidades existentes no parque, evidenciando as notificações que foram formalizadas e enviadas aos responsáveis pelos ativos.

m) A CONTRATADA deverá empenhar todos os esforços para garantir os indicadores nos níveis de conformidade definidos pela CONTRATANTE, formalizando, notificando e sensibilizando as equipes envolvidas.

2.11.4. IDENTIFICAÇÃO, DESENVOLVIMENTO, IMPLEMENTAÇÃO E MANUTENÇÃO DE PROCESSOS CORPORATIVOS

A CONTRATADA deverá utilizar-se de frameworks como o NIST Cyber Security Framework, CIS Controls, ISA/IEC 62443, juntamente com os padrões de segurança da série ISO/IEC 27000, como uma base para transmitir as pessoas adequadas, processos e tecnologia necessários para suportar o ciclo de vida da segurança dentro da contratante e auxiliar na manutenção dos processos corporativos com foco em segurança.

2.11.5. MONITORAMENTO EXTERNO, AMBIENTE WEB

a) Monitoramento de repositórios públicos (pastebin, github, etc.) visando detectar informações confidenciais e forma pública, como trechos de código-fonte, logins e senhas etc;

b) Detecção de sites de phishing ou que personificam a marca da CONTRATANTE e tentativa de eliminação;

c) Monitoramento em todas as camadas da WEB (surface, deep e dark-web) para detecção de possíveis ameaças e/ou vazamentos;

d) Monitoramento de uso indevido ou fraudulento da marca;

e) Monitoramento de domínio similares para execução de fraude;

f) Monitoramento de aplicativos falsos e disponibilizados em lugares como Google Play e Apple Store.

2.11.5. MONITORAMENTO INTERNO E TESTES

a) Avaliações em endpoints com antivírus medindo a segurança;

b) Avaliação da segurança em redes e Wi-Fi;

c) Varredura automática de ativos;

d) Scanner de vulnerabilidades Web (DAST), deverá ter dashboard de acompanhamento e comparativo da evolução da segurança, permitir a análise e reexecuções por demanda.

e) Baseline e conformidade dos ativos (hardening);

f) Ataques físicos contra a infraestrutura da contratante e os órgãos da administração;

g) Ataques físicos de engenharia social na infraestrutura da contratante e os órgãos da administração;

h) Analisar, tratar e responder aos eventos e incidentes de segurança cibernética, oriundos de ferramentas de monitoração e detecção de ataques, relatórios técnicos, e-mails, usuários e outros canais de entrada, inclusive externos;

i) Investigação forense, como de pessoas (fraudadores, crackers etc.) ou de sistemas computacionais e de redes de dados, como também outros serviços forenses que envolvam obtenção de evidências materiais e não materiais (como de computadores, unidades de armazenamento de dados e redes de comunicação de dados) visando identificar fraudes e golpes praticados contra a contratante e os órgãos da administração;
j) Realizar respostas aos incidentes cibernéticos decorrentes de vulnerabilidades sistêmicas;
k) Vigilância de meios de comunicação e análise de dados dos crackers e fraudadores;
l) Realizar a comunicação com outros CSIRT's, órgãos como CERT.br, CTIR, NIC, USCERT, entre outros, quando necessário;
m) Prover todos os alertas possíveis assim como recomendações para solução de falhas de "dia- zero"
n) Avaliação das políticas de backup e restore.

2.11.7. SERVIÇO PARA VARREDURAS DE VULNERABILIDADES

a) Deverá permitir a varredura de vulnerabilidades de todos os sistemas operacionais mencionados, equipamentos e demais dispositivos de diferentes fabricantes e não apresentar restrições, nem limitações quantitativas para varreduras conforme lista de referência de equipamentos e serviços no ambiente da contratante e os órgãos da administração.
b) Deverá ser capaz de analisar toda a infraestrutura de TI da CONTRATANTE e seus clientes conforme descritivos e quantitativos informados.
c) O serviço proposto para varredura de vulnerabilidades deverá ser capaz de analisar os diversos gerenciadores de banco de dados conforme quantitativos de referência informados, independente de fabricante, modelo ou versão, não sendo necessárias varreduras dos bancos de dados efetivamente.
d) As aplicações WEB CONTRATANTE e seus clientes, deverão ser analisadas para vulnerabilidades em seus serviços (por exemplo IIS, Apache, Tom Cat, Glassfish), infraestrutura onde a aplicação é executada.
e) A solução deverá ser capaz de verificar vulnerabilidades em gerenciadores de virtualização como Hyper-V e VMware;
f) A solução deverá apresentar capacidade para análise de vulnerabilidades na estrutura do Active Directory (AD);
g) A solução deverá ser capaz de prover a autenticação através de autenticação via AD (Active Directory) ou LDAP;
h) A solução deverá ser escalável em quantidade de varreduras de vulnerabilidades possíveis, suportando eventual crescimento do parque computacional da CONTRATANTE sem que haja necessidade de mudança de ferramenta para suportar tal crescimento ou demanda;
i) Deve ter a capacidade de detecção de bug chain e vulnerabilidades de lógica e de regras de negócio, exemplo IDOR).
j) A solução deverá permitir desenvolvimento e adequação a necessidades particulares da contratante e os órgãos da administração, permitindo a inclusão de testes sobre as plataformas específicas.

2.11.8. CARACTERÍSTICAS TÉCNICAS PARA OS SERVIÇOS DE VARREDURA DE VULNERABILIDADES

a) Todos os scanners devem ser administrados por um Gerenciador único.
b) O serviço deve possuir capacidade de receber atualizações em horários programados.
c) O serviço deve suportar vários scanners conectados simultaneamente.
d) O serviço deve possuir capacidade de atualizar os scanners automaticamente.
e) O serviço deve receber a atualização automática da base de vulnerabilidades.
f) O serviço deve possuir uma base de vulnerabilidades fornecida pelo fabricante, que deve ser atualizada de forma incremental diretamente do site do fabricante.

g) O serviço deve possuir uma base de análises que permite identificar vulnerabilidades CVE.
h) O serviço deve possuir em sua base de vulnerabilidades, para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, (CVE, CWE, BugTraq ou outra fonte), solução e link para o download da correção (se aplicável), contramedidas (se aplicável), informação e apresentação do exploit.
i) Se necessário, o scanner do serviço deve funcionar sem necessidade de acesso à internet.
j) O serviço deve prover o registro de atividades (logs) para fins de auditoria, no mínimo para os eventos de: data e hora, endereço IP da origem da conexão, identificação do usuário e atividades executadas na ferramenta.
k) O serviço deve prover interface gráfica WEB para gerenciamento de todos os seus componentes e suas configurações.
l) O serviço deve possuir suporte ao IP (Internet Protocol) versão 4 e versão 6.

2.11.9. REQUISITOS TÉCNICOS DO SERVIÇO DE VARREDURA DE VULNERABILIDADES

a) Serão aceitos serviços em forma de "appliance", "virtual appliance" ou software para instalação em máquina virtual.
b) Deverá o serviço estar disponível em sua última versão disponível e contar com suporte integral.
c) Não poderá o serviço estar em versão beta ou não contar com suporte do fabricante para versão definida.
d) O serviço deverá permitir a descoberta dos ativos da rede (servidores, ativos de rede ou serviços que possuam endereço IP) sem a necessidade de agentes para esse fim.
e) O serviço deverá ter capacidade de realizar automaticamente (através de agendamento automático) a descoberta de ativos;
f) O serviço deve ter um console que permita um gerenciamento centralizado de relatórios e análises de vulnerabilidades dos servidores ou ativos de rede que possuam endereço IP ou que sejam alocados no escopo desta contratação.
g) Permitir detectar vulnerabilidades em servidores Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.
h) Permitir verificar vulnerabilidades em ambiente Windows para, no mínimo:
1. Detecção de hotfixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus.
i) Suportar efetuar varredura à procura de vulnerabilidades e exploits.
j) Integrar-se com base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures).
k) Possuir módulos de varredura diferenciados para análise mais intrusiva enão intrusiva.
l) Efetuar varredura por endereço IP, range de IP, agrupamento de ativos, nome NetBIOS ou CIDR Notation.
m) O serviço deve possuir a capacidade de agendar varreduras de vulnerabilidades.
n) O serviço deve ser capaz de executar varreduras de vulnerabilidades sob demanda.
o) O serviço deve possibilitar a interrupção de uma varredura de vulnerabilidades, em qualquer momento da operação.
p) O serviço deve ser capaz de emitir notificação por e-mail quando uma varredura de vulnerabilidades terminar.
q) O Gerenciador deve possibilitar a configuração de desempenho na varredura de vulnerabilidades, como por número de conexões simultâneas ativos simultâneos.
r) O serviço deve permitir a integração com as API 's da Amazon e Microsoft Azure de serviços em cloud, a fim de descobrir imagens, ativas ou paradas, sem necessidade de escaneamento de rede.
s) Possuir capacidade de definir o número de alvos (IPs) para scannear simultaneamente e a velocidade de forma a não impactar o desempenho da rede.
t) Deve permitir o cadastramento de credenciais utilizadas para escaneamento para que seja permitido o uso de

tais credenciais para futuros escaneamentos, sem que o administrador da ferramenta saiba a senha destas credenciais.
u) O serviço deve possibilitar a integração com pelo menos 1 (uma) solução de cofre de senhas para recuperação automática de credenciais no momento da execução do escaneamento.
v) O serviço deve permitir a varredura de PII (Personable Identifiable Information) a fim de buscar informações sensíveis como, por exemplo, números de cartão de crédito em arquivos de texto.
w) O serviço deve permitir escaneamentos específicos, utilizando no mínimo os seguintes grupos de auditoria:
1. Deve possuir templates para varredura de vulnerabilidades mobile
2. Deve possuir templates para varredura de vulnerabilidades webapplication
3. Deve possuir templates para varredura de vulnerabilidades patch audit
4. Deve possuir templates para varredura de vulnerabilidades de acordo CIS
5. Deve possuir templates para varredura de vulnerabilidades de acordo PCI
6. Deve possuir condição de criação de modelos específicos com base no levantamento automatizado.
x) Este mecanismo deve possibilitar a visualização de todos os patches disponíveis para um determinado host e permitir a visualização destes patches por tipo de patch, como críticos, atualizações de segurança, importantes etc.
y) O serviço deve possuir padrões de varredura de conformidade ou "benchmarking" pelo menos nos padrões: DISA Gold Disk, SCAP, NIST, FDCC,USGCB, CIS, Microsoft etc.
z) O serviço deve prover modelo de validação de conformidade para a Norma PCI DSS.
aa) O serviço deve ser capaz de criar internos tickets para tratamento de vulnerabilidades, e distribuir estes para os usuários da solução.
bb) O serviço deve ser capaz de enviar e-mails para criação de tickets externos para tratamento de vulnerabilidades em ferramentas de ITSM externas.
cc) O serviço deve ser compatível pelo menos com os seguintes sistemas operacionais:
1. Windows Server 2008 SP2 ou maior (32-bits e 64-bits)
2. Windows 7 (32-bits e 64-bits)
3. Windows Server 2008 R2 SP1 ou maior (64-bits)
4. Windows 8 (32-bits e 64-bits)
5. Windows Server 2012 (64-bits)
6. Windows 8.1 (32-bits e 64-bits)
7. Windows 10 (32-bits e 64-bits)
8. Windows Server 2012 R2 (64-bits)
9. Windows Server 2016 (64-bits)
10. Windows 11
11. Linux
12. MacOS

2.11.10. POLÍTICAS E PROCEDIMENTOS

Confecção de políticas e procedimentos de segurança cibernética devendo cobrir com detalhes temas como:
1. Desenvolvimento Seguro
2. Segurança em Recursos Humanos
3. Gestão de Prestadores de Serviços e Parceiros
4. Gestão de Ativos
5. Criptografia
6. Política Geral de Segurança Informação

7. Programa de Conscientização de Segurança da Informação Uso Aceitável
8. Privacidade de Dados Pessoais
9. Perímetros de Segurança Eletrônica
10. Resposta a Incidentes
11. Gerenciamento de Mudanças

2.11.11. FORMA DE TRABALHO

a) A abordagem da CONTRATADA à segurança da informação deverá ser "TOP-DOWN", ou seja, alinhada aos negócios para fornecer rastreabilidade e justificativa para controles de segurança - técnicos e não técnicos.
b) As práticas de segurança da informação e gestão de risco devem ser simples, apropriadas e economicamente proporcionais para garantir que o esforço e os recursos sejam empregados de acordo.
c) Essa abordagem holística à segurança da informação garante conformidade com todos os padrões e estruturas de melhores práticas, além de influências internas e externas de segurança.
d) Essas metodologias comprovadas apresentam arquiteturas sólidas de segurança para proteger contra as ameaças mais recentes e avançadas, ao mesmo tempo em que fornecem ambientes ágeis e flexíveis que permitem e suportam iniciativas de negócios.

2.12. SERVIÇO DE TREINAMENTO

2.12.1. Características Gerais:

a) Serviços contemplados:
Serviços de Workshop para de conscientização para Segurança da informação;
b) Deverá ser proposto um plano de treinamento sobre segurança cibernética, visando melhorar a cultura de segurança da CONTRATANTE. O plano deverá respeitar a tabela de quantitativo ora apresentada neste Termo de Referência. Este plano terá como entregável:
1. Diagnóstico de levantamento das necessidades;
2. Definição dos objetivos do treinamento;
3. Definição com a CONTRATANTE, do formato de cada treinamento (EAD / Presencial);
4. Conteúdo que será disponibilizado a CONTRATANTE, utilizando como base o item: (Características do Treinamento) explícita neste Termo de Referência;
5. Proposição de cronograma para cada treinamento, com periodicidade trimestral;
6. Teste de absorção do conhecimento através de prova de certificação;
7. Reciclagem de conteúdo de aprendizagem com periodicidade mínima de 6 meses.

2.12.2. REQUISITOS DE NEGÓCIO

a) A CONTRATANTE busca serviços de treinamento em segurança da informação, para trazer maior proteção aos colaboradores da CONTRATANTE.
b) Devem ser baseados nas ferramentas de segurança da CONTRATANTE e da CONTRATADA para realização do serviço de treinamento.
c) Conforme definição da CONTRATANTE, a CONTRATADA deverá ser responsável pelo Serviço de Treinamento em Segurança da Informação.

2.12.3. Referente ao item 1:

a) A CONTRATANTE estima a utilização de 16 (dezesseis) unidades de treinamento, que equivalem a 03 turmas/trimestre, durante a vigência do contrato.
b) Estes serviços de treinamento deverão ser executados em modelo 8x5. Entende-se por horário de atendimento

8x5 de segunda a sexta, a partir de 08:00 até às 17:00.

2.12.4. CARATERÍSTICAS DOS TREINAMENTOS

A CONTRATADA deverá realizar, através de serviços de treinamento, o repasse das recomendações e melhores práticas dos serviços executados neste contrato à CONTRATANTE.

2.12.5. DESCRIÇÃO DOS SERVIÇOS

2.12.5.1. SERVIÇO DE WORKSHOP PARA SEGURANÇA DA INFORMAÇÃO ATÉ 05 PESSOAS/TURMA

a) A CONTRATADA deve prover serviço de workshop com carga horária de até 40 horas, contemplando 04 trilhas de conhecimento, tendo o seguinte escopo mínimo:
1. Workshop Para Segurança da Informação Executivos
2. Workshop Para Segurança da Informação Usuários Comuns
3. Workshop Para Segurança da Informação Analistas
4. Simulação em ataques e sala de crise
b) Os treinamentos serão ministrados em Língua Portuguesa.
c) Teste de absorção do conhecimento através de prova de certificação.
d) Emissão de certificação pela contratada mediante assertividade mínima de 80% no teste de absorção.
e) Deverá haver teste de avaliação de conhecimento.
f) Emissão de certificação pela contratada mediante assertividade mínima de 80% no teste de avaliação de conhecimento.
g) Não serão aceitas aulas gravadas.
h) Os treinamentos deverão serem ministrados nas dependências da CONTRATANTE.

2.12.5.2. CONTEÚDO PROGRAMÁTICO

2.12.5.2.1. Grupo 1: Executivos

a) Introdução à Segurança da Informação:
1. Conceitos básicos de segurança da informação.
2. Importância da segurança da informação para a empresa.
b) Riscos e Ameaças Cibernéticas:
1. Identificação e compreensão das principais ameaças cibernéticas.
2. Análise do impacto potencial de violações de segurança.
c) Normas e Regulamentações:
1. Visão geral das principais normas e regulamentações de segurança da informação (ex: ISO 27001, GDPR, LGPD).
2. Implicações legais e de conformidade para a organização.
d) Gestão de Incidentes de Segurança:
1. Procedimentos para lidar com incidentes de segurança da informação.
2. Papel dos executivos na resposta a incidentes.
e) Conscientização em Segurança:
1. O papel dos executivos na promoção de uma cultura de segurança.
2. Estratégias para envolver e educar os colaboradores em relação à segurança.

2.12.5.2.2. Grupo 2: Usuários Comuns

a) Práticas de Segurança Básicas:

1. Senhas fortes e seguras.
2. Atualizações de software e sistema operacional.
b) Phishing e Engenharia Social:
1. Reconhecimento e prevenção de ataques de phishing.
2. Como identificar tentativas de engenharia social.
c) Uso Seguro de Dispositivos Móveis:
1. Boas práticas para proteger dispositivos móveis.
2. Gerenciamento de aplicativos e permissões.
d) Navegação Segura na Internet:
1. Dicas para evitar sites maliciosos e downloads não seguros.
2. Uso de conexões seguras (HTTPS).
e) Sensibilização para Redes Sociais:
1. Riscos de segurança associados ao uso de redes sociais.
2. Proteção de informações pessoais.

2.12.5.2.3. Grupo 3: Analistas
a) Análise de Vulnerabilidades:
1. Técnicas de análise de vulnerabilidades em sistemas e redes.
2. Identificação e classificação de vulnerabilidades.
b) Testes de Intrusão (Penetration Testing):
1. Planejamento e execução de testes de intrusão éticos.
2. Relatórios e recomendações pós-teste.
c) Monitoramento e Detecção de Ameaças:
1. Uso de ferramentas de monitoramento para identificar atividades suspeitas.
2. Análise de logs e eventos de segurança.
d) Resposta a Incidentes de Segurança:
1. Procedimentos de resposta a incidentes.
2. Isolamento e contenção de ameaças.
e) Gerenciamento de Políticas de Segurança:
1. Desenvolvimento e implementação de políticas de segurança.
2. Monitoramento e revisão periódica das políticas.

2.12.5.2.4. Grupo 4: Simulação em ataques e sala de crise
1. Fundamentos e Simulações
2. Gerenciamento de Crises
3. Exercício Prático e Melhorias Contínuas

2.13. CONDIÇÕES GERAIS DOS SERVIÇOS PRESTADOS
a) Relatórios sobre a prestação dos serviços:
1. A CONTRATADA fornecerá relatórios mensais sobre a prestação dos serviços, em papel e em arquivo eletrônico, preferencialmente em formato PDF, com informações analíticas e sintéticas sobre os serviços realizados, incluindo-se requisições abertas e fechadas, enfatizando aqueles resolvidos no período.
2. Constarão dos relatórios dados de todos os chamados ocorridos no período, data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

a) Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da tabela abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas a seguir:

	NÍVEL DE SEVERIDADE DO CHAMADO			
	BAIXA	**MÉDIA**	**ALTA**	**URGENTE**
Descrição do chamado	Problema técnico que gera pouco ou baixo Impacto na utilização do serviço	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo o uso do serviço	Problema técnico que impeça completamente a utilização de uma funcionalidade do serviço	Problema técnico que impeça a utilização do serviço em sua totalidade
Início de Prazo para o atendimento da ocorrência	Até 24 horas corridas	Até 12 horas corridas	Até 04 horas corridas	Até 02 horas corridas
Percentual de Chamados (Meta)	85%	90%	92%	90%
Multa	0,5% do valor mensal	1% do valor mensal	1,5% do valor mensal	2% do valor mensal
Limite de Penalidade	Até 5% do valor total do contrato ao longo dos 15 meses	Até 5% do valor total do contrato ao longo dos 15 meses	Até 5% do valor total do contrato ao longo dos 15 meses	Até 5% do valor total do contrato ao longo dos 15 meses

TABELA NÍVEL DE SEVERIDADE DO CHAMADO

c) A medição dos SLAs de serviço será feita usando a seguinte fórmula:

9. Meta = Qtde de registros atendidos no prazo / Total de registros atendidos no prazo.

d) Em caso de problemas de falhas de software (bugs), cujo serviço dependa da liberação de nova versão ou patches de correção do software pelo fabricante, a CONTRATADA deve providenciar uma solução de contingência para o serviço, no prazo máximo de 90 (noventa) dias úteis contados a partirda abertura do chamado.

e) A solução de contingência não caracterizará a conclusão de um chamado, contudo suspenderá a contagem de tempo para a resolução de ocorrência.

f) A CONTRATADA deverá assegurar a assistência técnica necessária à satisfatória utilização dos serviços, no que consiste à instalação, reinstalação e atualização de softwares/firmwares de qualquer solução que esteja empregada na prestação destes serviços aqui descritos.

g) Entende-se por manutenção corretiva a série de procedimentos destinados ao restabelecimento operacional do serviço com todas suas funcionalidades, compreendendo, inclusive, atualização de softwares por um substituto de igual ou maior configuração, ajustes, reparos, correções necessárias e todas as configurações solicitadas pela CONTRATANTE.

MÉTRICAS

Unidade Riscos de Terceiros
01 (uma) Unidade Riscos dos Terceiros deverá contemplar:
- 50 registros CNPJ

Unidade SOC
01 (uma) Unidade SOC deverá contemplar:
- 50 dispositivos monitorados

Unidade NOC
01 (uma) Unidade NOC deverá contemplar:
- 50 dispositivos monitorados

Unidade NDR
01 Unidade – NDR deverá contemplar:
- Throughput de até 02Gbps;
- Capacidade de analisar e identificar até 7.500 dispositivos;
- Suportar e analisar até 50.000 conexões por minuto.

Dispositivos Linux
01 (uma) unidade Linux deverá contemplar:
- 30 dispositivos monitorados

Unidade Cripto
01 (uma) unidade Cripto deverá contemplar:
- 50 dispositivos monitorados

Unidade Domínio
01 (uma) unidade Domínio deverá contemplar:
- 30 Domínio de monitoramento

Unidade Usuário
01 (uma) unidade Usuário deverá contemplar:
- 100 usuários

Turmas / Ano
01 (uma) unidade Turmas / Ano deverá considerar:
- Até 05 alunos