



PROPOSTA COMERCIAL

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

EDITAL DE PREGÃO ELETRÔNICO n. 21/2022

O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação, através da seleção de empresa especializada, para o fornecimento de Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Brasília, dia 22 de março de 2022

**Matriz: Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES – CEP: 29.050-360
Tel: +55 27 3334.8900 - Fax: +55 27 3334.8905 – www.ish.com.br
CNPJ: 01.707.536/0001-04 – Ins. Est: 082.338.03-5**



Brasília, dia 22 de março de 2022

A

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Ref.: EDITAL DE PREGÃO ELETRÔNICO n. 21/2022

Prezados Senhores,

*Atendendo à convocação do edital que rege a licitação na modalidade **EDITAL DE PREGÃO ELETRÔNICO n. 21/2022**, promovido pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**, a empresa **ISH Tecnologia S/A**, a seguir identificada, apresenta, neste volume único, a proposta de preços cotada para atendimento do objeto deste certame.*

Declaramos nosso interesse e prioridade conferida ao desenvolvimento do projeto ora proposto, assim como nosso comprometimento de que serão oferecidas as garantias necessárias para sua adequada execução, incluindo o envolvimento de equipe, recursos de contrapartidas previstos e outras condições específicas definidas nesta proposta.

*Ficamos lisonjeados com a possibilidade de participar deste processo e estamos convictos de que a **ISH Tecnologia S/A**, tem total capacidade de fornecer o melhor serviço, dentro das melhores condições de qualidade, custo e prazo para **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA***

Atenciosamente,

Hélio Ferreira da Silva Júnior
Executivo de Negócios
ISH TECNOLOGIA S/A
CNPJ: 01.707.536/0001-04



PROPOSTA COMERCIAL

***MINISTÉRIO DA JUSTIÇA E SEGURANÇA
PÚBLICA***

EDITAL DE PREGÃO ELETRÔNICO n. 21/2022

IDENTIFICAÇÃO DA EMPRESA

Matriz: Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES – CEP: 29.050-360
Tel: +55 27 3334.8900 - Fax: +55 27 3334.8905 – www.ish.com.br
CNPJ: 01.707.536/0001-04 – Ins. Est: 082.338.03-5



IDENTIFICAÇÃO DA EMPRESA

Razão Social:	ISH TECNOLOGIA S/A.
Endereço:	Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES;
CEP:	29.050-360
Fone:	(27) 3334-8900 / (27) 3334-8905
Fax:	(27) 3334-8900 / (27) 3334-8905
CNPJ/MF:	01.707.536/0001-04
Inscrição Estadual:	082.338.03-5
Registro na Junta Comercial:	20050336460
Site na Internet:	www.ish.com.br

Dados Bancários:

INSTITUIÇÃO	ENDEREÇO/AGÊNCIA	TELEFONE
1) BANCO DO BRASIL Nº 001	Praia do Canto - Vitória/ES Agência 1802-3 C/C 20.050-6	(27) 3335-3800
2) Banco BRADESCO Nº 237	Praia do Canto – Vitória/ES Agência 3511-5 C/C. 1924-0	(27) 3232-7500
3) Banco ITAU Nº 341	Praia do Canto – Vitória/ES Agência 0870 C/C 45.307-5	(27) 3003-8766
4) Banco SANTANDER Nº 033	Centro – Vitória/ES Agência 3874 C/C 13.000653-4	(27) 3198-4271

Dados do Representante Legal:

Nome:	Hélio Ferreira da Silva Junior
Estado Civil:	Casado
Profissão:	Executivo de Negócios
CPF:	003.868.541.81
Carteira de Identidade:	2.107.159 SSP/DF
Cargo:	Executivo de Negócios
E-mail:	Helio.ferreira@ish.com.br
Endereço:	Rua 31 sul LT 09 Ed. Mozart Apto. 1510 Águas Claras

Matriz: Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES – CEP: 29.050-360
Tel: +55 27 3334.8900 - Fax: +55 27 3334.8905 – www.ish.com.br
CNPJ: 01.707.536/0001-04 – Ins. Est: 082.338.03-5



Declaração Geral

A
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Ref.: EDITAL DO EDITAL DE PREGÃO ELETRÔNICO n. 21/2022

A ISH Tecnologia S/A., sob CNPJ nº 01.707.536/0001-04, sediada à Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES; por meio de seu representante legal Diretor Executivo, o Sr. Vitor Teixeira Costa, portador da Carteira de Identidade nº 2.142.312- SSP/DF e CPF nº 990.365.091-49; **DECLARA que nos preços cotados já estão incluídos todos os custos incidentes, tais como: salário, ônus tributários, fiscais, parafiscais, trabalhistas e sociais, seguro, transporte, instalação, configuração, suporte técnico, com deslocamento, hospedagem e alimentação do suporte técnico, inclusive com a desmontagem, montagem e transporte para fins de reparos ou de substituição durante o período do suporte técnico e demais despesas de qualquer natureza que possam incidir, direta ou indiretamente, sobre o objeto do Termo de Referência.**

Brasília, dia 22 de março de 2022

Hélio Ferreira da Silva Júnior
Executivo de Negócios
ISH TECNOLOGIA S/A
CNPJ: 01.707.536/0001-04



PROPOSTA COMERCIAL

***MINISTÉRIO DA JUSTIÇA E SEGURANÇA
PÚBLICA***

EDITAL DE PREGÃO ELETRÔNICO n. 21/2022

Proposta de Preço

Matriz: Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES – CEP: 29.050-360
Tel: +55 27 3334.8900 - Fax: +55 27 3334.8905 – www.ish.com.br
CNPJ: 01.707.536/0001-04 – Ins. Est: 082.338.03-5



Proposta de Preços

PREGÃO ELETRÔNICO Nº 021/2022
(Processo Administrativo nº 08006.000003/2021-38)

Objeto: Contratação de empresa especializada, para o fornecimento de **Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team**, pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, de acordo com as especificações técnicas contidas do Termo de Referência – TR e seus anexos.

À COORDENAÇÃO DE PROCEDIMENTOS LICITATÓRIOS

Em atendimento ao Edital do Pregão em epígrafe, apresentamos a seguinte proposta de preços:

Grupo	item	Codigo Siasg Catser	Descrição do Bem ou Serviço	QTD	Metrica ou Unidde de medida	Valor Unit (R\$)	Valor Mensal (R\$)	Valor Total (24 Meses) (R\$)
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	-	R\$ 46.666,66	R\$ 1.119.999,84
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	-	R\$ 49.083,33	R\$ 1.177.999,92
Valor Global (somatório do Valor Total 24 meses)								R\$ 2.297.999,76

Dados da Empresa
Razão Social: ISH TECNOLOGIA S/A.
CNPJ (MF) nº 01.707.536/0001-04
Representante (s) legal (is) com poderes para assinar o contrato: Vitor Teixeira Costa
CPF: 990.365.091-49 RG: 2142312 SSP/DF
Inscrição Estadual nº 082.338.03-5
Endereço Completo (com CEP): Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES; CEP 29.050-360
Telefone: (27) 3334-8900 / (27) 3334-8905 / (61) 98588-8888
E-mail: helio.ferreira@ish.com.br
Dados Bancários (Banco do Brasil nº: 001, agência nº 1802-3, CC: 20.050-6) Praça: Vitoria

Matriz: Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES – CEP: 29.050-360
Tel: +55 27 3334.8900 - Fax: +55 27 3334.8905 – www.ish.com.br
CNPJ: 01.707.536/0001-04 – Ins. Est: 082.338.03-5



Contato: Fone: (27) 3335-3800

Declarações

Validade da Proposta (mínimo 60 dias), conforme o artigo 64, § 3º da Lei 8.666/93.:

Declaramos que nos preços propostos estão incluídos todos os custos e despesas de qualquer natureza, incidentes sobre os objetos desta proposta.

Declaramos total conhecimento e concordância dos termos do edital do pregão e dos seus anexos.

Assinatura

Local e data: 14/03/2022

Nome do Representante Legal: Hélio Ferreira da Silva Junior

Identidade do Representante Legal: 2.107.159 SSP/DF

Hélio Ferreira da Silva Júnior
Executivo de Negócios
ISH TECNOLOGIA S/A
CNPJ: 01.707.536/0001-04

CADERNO TÉCNICO

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

PREGÃO ELETRÔNICO nº 21/2021

ISH TECNOLOGIA S/A



1. REFERENTE AO OBJETO DA LICITAÇÃO

Contratação de Serviços Gerenciados de Segurança da Informação para o Ministério da Justiça e Segurança Pública.

2. SERVIÇO PROPOSTO

Esta proposição contempla todo os serviços do Grupo 1 solicitado pelo MJSP, conforme descrito a seguir.

2.1. Escopo

Detalhamos abaixo o escopo de fornecimentos dos itens previstos no edital.

Grupo	Item	Código SIASG CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade de medida
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)

2.1.1. GRUPO 1: ITEM 1 - SERVIÇO DE SECURITY OPERATIONS CENTER - SOC

O SOC da ISH TECNOLOGIA funcionará 24 horas por dia e 7 dias por semana, para sustentar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério da Justiça e Segurança pública, bem como realizar permanentemente ações proativas voltadas para a segurança do parque computacional do Ministério da Justiça e Segurança Pública, sem prejuízo aos níveis de serviços definido neste Termo de Referência, bem como realizando as seguintes atividades, não se restringindo somente a elas:

A ISH TECNOLOGIA fará o monitoramento contínuo e análise, predizendo, prevendo, prevenindo, detectando e respondendo efetivamente as ameaças de todos incidentes cibernéticos.

Gerará painéis dinâmicos e em tempo real da situação atual de segurança do Ministério informando através de um score o nível de segurança.

Atuará como suporte de primeiro nível aos incidentes cibernéticos identificando, classificando, interrompendo, catalogando todas as tentativas de ataque aos sistemas e à infraestrutura do ministério.

Comunicará tempestivamente a MJSP medidas a serem tomadas para evitar ou conter incidente.

Atuará no sentido de interromper um incidente quando a equipe do NOC ou suporte N1, N2 e N3 estiver limitada contratualmente ou em sua capacidade operacional. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team.

Outros serviços os quais o SOC em substituição ao NOC, não definidos inicialmente nos protocolos do item anterior, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a MJSP e a ISH TECNOLOGIA.

Atuará em harmonia com o NOC do ministério.

A IST TECNOLOGIA prestará o serviço de SOC realizando a detecção, triagem, investigação e resposta a incidente de eventos utilizando Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério de acordo com as seguintes funções:

Na camada de Automação:

Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR);

Camada de Análise e Correlacionamento:

Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR);

Análise de Tráfego de Rede (Network Traffic Analysis - NTA);

Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA);

Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI);

Na camada de coleta:

Informações de segurança e gestão de eventos (Security Information and Event Management - SIEM).

Configuração, manutenção, monitoramento e operação da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

Monitoramento e Análise de toda a infraestrutura do Ministério, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Para o devido dimensionamento do esforço de trabalho necessário, atualmente, a Plataforma de SIEM/SOAR/NTA/UEBA/CTI coleta eventos que representam aproximadamente 200 GB/dia e 5000 EPS.

Realização de atividades de preparação do processo de coleta de logs, incluindo a normalização, filtragem, redução, agregação e priorização, bem como atividades que envolve o processamento, normalização, armazenamento, e demais atividades de correlacionamento de logs que serão realizadas nas ferramentas da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir dos dados disponibilizados pelo Ministério quando ocorrer a contratação.

Caso as ferramentas de propriedade do Ministério não atendam a completa execução dos serviços objeto da presente contratação a ISH TECNOLOGIA poderá adotar solução tecnológica complementar em termos de hardware e software.

A ISH TECNOLOGIA poderá utilizar soluções de hardware e software proprietárias desde que previamente autorizadas pelo MJSP, arcando a ISH TECNOLOGIA com todos os custos diretos e indiretos inerentes a utilização de solução tecnológica e seus licenciamentos necessários.

O SOC da ISH funcionará como o centralizador de todas as informações de segurança da informação e suporte de primeiro nível para os processos previstos no item 4.1.9.4 do certame, por isso, a necessidade de seu funcionamento será ininterrupto. O dimensionamento da equipe do SOC será a cargo da ISH TECNOLOGIA em quantitativo mínimo que garanta o monitoramento ininterrupto de seu funcionamento, a qualidade das informações prestadas e estar apta e atuará no estado da arte em termos de segurança da informação, assim como cumprir os Níveis Mínimos de Serviço Exigidos determinados.

Segue as principais atividades que serão executadas de forma contínua pela ISH TECNOLOGIA:

Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;

Priorizar os atendimentos críticos, conforme definição do MJSP;

Monitorar de forma permanente e avaliar criticamente os produtos e serviços de segurança do MJSP;

Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;

Supervisionar sua equipe na execução dos serviços de Security Operations Center e Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team;

Elaborar e propor plano de execução dos serviços;

Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços;

Executar outros serviços correlatos à supervisão dos profissionais na execução dos serviços;

Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;

Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do Ministério da Justiça e Segurança pública, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;

Consolidar os relatórios de atividades mensais (mês calendário), referente aos serviços, provendo informações gerenciais ao MJSP;

Supervisionar sua equipe de profissionais na execução das ações conjuntas com a área de infraestrutura, cumprindo a política de segurança da informação do Ministério e aplicando as melhores práticas de segurança;

Consolidar todas as soluções adotadas na execução das atividades em manuais de procedimentos e em base de conhecimento;

Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração. O processo de auditoria do MJSP é contínuo;

Implantar as melhorias solicitadas pelos servidores do MJSP através das aberturas de chamados no sistema de gestão de serviços de TI;

Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do MJSP na gestão de segurança da informação;

Aplicar as práticas do ITIL 3 ou superior.

Manter atualizado o Configuration Management Database (CMDB) na ferramenta de Gerenciamento de Serviços de TI utilizada pelo MJSP ou fornecida pela ISH TECNOLOGIA sem custo adicional, quanto aos recursos administrado;

Consolidar as sugestões de melhoria;

Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação do MJSP;

Subsidiar tecnicamente, quando demandado, os processos de aquisição;

Subsidiar os servidores do MJSP quanto ao dimensionamento da capacidade de hardware e configuração dos ativos de segurança;

Abrir chamados técnicos, na língua inglesa ou outro idioma quando necessário, para os serviços de suporte técnico remoto das soluções de hardware e software de TI do MJSP, quanto aos recursos administrados;

Avaliação do ambiente, serviços e sistemas, monitoramento contínuo, apoiar o MJSP na homologação de soluções de segurança e na execução de atividades de controle de acessos e demais serviços relacionados à Segurança da Informação no ambiente tecnológico do MJSP.

Instalar ou customizar softwares aplicativos e equipamentos relacionados aos serviços, objeto desse TR, homologados para uso no Ministério da Justiça, por solicitação do MJSP;

Receber as diretrizes relacionadas à área de Segurança da Informação e providenciar a execução e alocação de recursos de trabalho;

Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo MJSP;

Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo MJSP;

Consolidar em manuais e scripts todos os serviços e soluções adotadas sejam eles novos ou já implantados no MJSP;

Auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento dos mesmos pelas demais áreas de TI;

Apoiar o MJSP na análise e definição das regras de uso dos recursos computacionais do MJSP;

Implantar as melhorias solicitadas pelos servidores do MJSP através das ordens de serviço;

Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;

Monitorar o ambiente lógico da MJSP identificando de forma proativa possíveis tentativas ou ataques aos ativos da MJSP;

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;

Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;

Implantar e configurar regras na Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério;

Realizar análise de tentativas de invasão a sistemas e equipamentos;

Auxiliar o MJSP nos projetos de Segurança da Informação;

Propor procedimentos de Segurança da Informação;

Apoiar o MJSP na revisão e atualização da política de segurança da informação;

Executar periodicamente testes de alta disponibilidade na infraestrutura do MJSP com o objetivo de validar o seu funcionamento;

Elaborar um plano de teste do ambiente de infraestrutura de segurança do MJSP, que deverá ser mantido atualizado continuamente. Este plano poderá servir de referência para elaboração de um Plano de Continuidade dos Serviços de Segurança da Informação;

Sugerir a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério;

Execução de mudanças de configuração nos ativos sob sua administração;

Executar medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da MJSP;

Execução das atividades relativas aos normativos e governança do MJSP naquilo que for relativo à sua área de atuação.

Os produtos listados abaixo serão criados pela ISH TECNOLOGIA e atualizados em conformidade com os padrões e necessidade do Ministério da Justiça:

Documento contendo a volumetria média de acessos, listando os limites a partir do qual serão considerados um incidente cibernético;

Guia de procedimentos de sustentação do serviço de proteção de e-mail;

Guia de procedimentos de sustentação do serviço de antivírus;

Guia de procedimentos de sustentação do serviço de proteção unificada;

Guia de procedimentos de sustentação do serviço de gestão unificado de ameaças;

Guia de procedimentos de sustentação do serviço de firewall de aplicação;

Guia de procedimentos de sustentação do serviço de gerenciamento de vulnerabilidades;

Relatórios de Continuidade de Negócios contendo indicadores de capacidade e disponibilidade dos ativos, além de projeções de elevação do uso dos recursos computacionais;

Documento contendo os requisitos de segurança da informação para a homologação e liberação de serviços, aplicações, servidores de rede;

Catálogo de Serviços e Base de Itens de Configuração;

Base de Conhecimento.

A ISH TECNOLOGIA permitirá ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criará novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou que precisam ser monitoradas;

A ISH TECNOLOGIA irá apoiar o MJSP em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;

A ISH TECNOLOGIA irá realizar a configuração das ferramentas que compõem as soluções sob sua administração, a fim de garantir o uso eficiente delas;

Sempre que houver atendimento, a ISH TECNOLOGIA enviará relatório de atividades por e-mail para o MJSP;

A ISH TECNOLOGIA irá acionar o fabricante das ferramentas, sob sua administração, sempre que necessário, sem nenhum custo adicional para o MJSP.

Monitoramento e Visibilidade

Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao Ministério da Justiça, através de correlacionamento de logs e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente cibernético, conforme definido em processo de gestão de incidentes.

O SOC será executado no ambiente da MJSP e/ou da ISH TECNOLOGIA.

Quando no ambiente da ISH TECNOLOGIA, atenderá os requisitos mínimos:

Estará localizado fisicamente em território nacional;

Utilizará sistema de gerenciamento de CFTV, que viabilizem o monitoramento de pessoas, equipamentos e sistemas relacionadas ao contrato do MJSP e cujas imagens possam ser recuperadas por no mínimo 90 (noventa) dias;

Efetuará registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;

Possuirá solução de monitoramento de disponibilidade e desempenho de seus ativos de TIC e de subsistemas;

O perímetro será protegido contra intrusão e acesso indevido;

Será vigiado fisicamente de forma ininterrupta por segurança especializada em regime de 24x7x365;

Terá controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;

Será configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

Terá sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;

Terá componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

Possuirá processos implementados que garantam a segurança das informações do MJSP, em conformidade com a norma ABNT NBR ISO/IEC 27001.

A ISH TECNOLOGIA irá disponibilizar à MJSP acesso de leitura aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

Quando no ambiente da MJSP, a ISH atenderá aos seguintes requisitos mínimos:

Possuirá solução de monitoramento de disponibilidade e desempenho de seus ativos de TIC e de subsistemas;

O perímetro lógico deve ser protegido contra intrusão e acesso indevido;

Será configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

Possuirá processos implementados que garantam a segurança das informações do MJSP, em conformidade com a norma ABNT NBR ISO/IEC 27001.

A ISH TECNOLOGIA disponibilizará à MJSP acesso de leitura aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

2.1.2. Grupo 1: Item 2 - Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team

O CISRT - Blue Team da ISH TECNOLOGIA funcionará de forma ininterrupta 24 horas por dia e 7 dias por semana, associado ao SOC para atividades de apoio ao suporte de primeiro nível e contenção de ataques, bem como, para atividades e suporte de segundo nível em diante e tendo por objetivos proativos prevenir, tratar, responder, além de objetivos reativos de analisar, documentar e indicar como conter e remediar os eventos de segurança da informação e de dados que foram transformados em um incidente cibernético, sem prejuízo aos níveis de serviços definido no certame deste caderno técnico.

A ISH TECNOLOGIA realizará avaliação completa do ambiente do MJSP com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do MJSP.

A análise dos controles de segurança será realizada obedecendo o framework de segurança cibernética do NIST.

A análise será conduzida por profissional com certificação CISSP – Certified Information Systems Security da ISH, que será responsável pela apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores de TI do Ministério da Justiça e Segurança pública.

A ISH observará as orientações e técnicas emanadas pelos padrões internacionais e pela Rede Federal de Gestão de Incidentes Cibernéticos, além de outros apresentados por ela mesmo, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

NIST Cybersecurity Framework, Version 1.1 ou mais recente;

NIST Privacy Framework, Version 1.0 ou mais recente;

NIST Special Publication 800-61 Revision 2 (Computer Security Incident Handling Guide);

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

NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations);

SANS Incident Handler's Handbook; 4.1.15.3.7. CIS Control, Version 7.1 ou mais recente;

ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management;

ISO/IEC 27035-2:2016 - Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response;

ISO/IEC 27035-3:2020 - Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations;

Incidente cibernético - ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso (Decreto Nº10.748, de 16 de julho de 2021 - Cap. I, Art.3º - V).

Para divulgação de ações de segurança da informação (Alertas, Conscientização e Recomendações) aos usuários finais, equipes de TIC e aos gestores com o objetivo de fortalecer uma estrutura para projetar, implementar, monitorar, manter e melhorar a segurança da informação consistente com a cultura organizacional, conforme preceitua a ABNT NBR ISO/IEC 27000, bem como para acompanhamento e avaliação dos indicadores de performance e serviços de SOC e CSIRT pelos gestores de TIC do Ministério a ISH TECNOLOGIA deverá desenvolver e manter um Portal WEB de CSIRT do Ministério, para a disponibilização de tais informações, como também informações para registro de notificações por usuários externos ao Ministério com uso de tecnologias seguras, definidas pela CRS, para comunicações através de canal seguro.

A seguir é apresentado a Tabela 7 com as categorias quanto a natureza, impacto ao negócio, impacto quanto as informações e esforço de recuperação de incidentes com o objetivo de definir o escopo dos serviços prestados pela ISH TECNOLOGIA;

Tabela 7 - Categorias quanto natureza do impacto

Natureza	Descrição da Natureza	Impacto ao Negócio	Descrição do Impacto ao negócio	Impacto quanto as informações	Descrição do Impacto quanto as informações	Esforço de Recuperação	Descrição do esforço necessário para a recuperação
Evento	Algo que ocorreu nos sistemas de informação, infraestrutura ou dados mas não necessariamente malicioso ou que requer uma ação.	Nenhum	Nenhum efeito na capacidade da organização de fornecer todos os serviços a todos os usuários	Nenhum	Nenhuma informação foi exfiltrada, alterada, apagada ou de outra forma comprometida	N/A	Não se aplica
Alerta	Algo potencialmente acionável. Uma indicação de um evento acionável.	Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu eficiência			Regular	O tempo para a recuperação é previsível com os recursos existentes
Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, mas sem impacto à missão ou ao negócio.	Médio	A organização perdeu a capacidade de fornecer um serviço essencial e crítico para um subconjunto de	Quebra de privacidade	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	Complementado	O tempo para a recuperação é previsível com recursos adicionais
				Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		
				Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas		
Incidente grave	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, com impacto à missão ou ao negócio.	Alto	A organização não é mais capaz de fornecer alguns serviços essencial e críticos a nenhum usuário e ou o comprometimento de dados institucionais e ou pessoais.	Quebra de privacidade	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	Estendido	O tempo para a recuperação é imprevisível; são necessários recursos adicionais e ajuda externa
Invasão e/ou Vazamento	Perda ou comprometimento de sistemas, dados regulados, propriedade empresarial que dispara uma ação ou resposta legal que vai além dos serviços de monitoramento e respostas a incidentes.			Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		
				Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas		
				Quebra de privacidade	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	Não Recuperável	A recuperação do incidente não é possível (por exemplo, os dados sensíveis exfiltrados e postados público); lançar investigação
Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas						
Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas						

O início do processo de resposta a incidente cibernético realizado pela ISH se dará, sempre que um evento adverso for detectado e descrito no presente termo de referência, porém não se limitando a este. Poderá o corpo técnico de segurança do MJSP também e a qualquer tempo, abrir um incidente de segurança, o qual deve seguir no mínimo o seguinte fluxo e requisitos:

Após o incidente aberto, a responsabilidade do grupo de resposta a incidente de segurança (CSIRT – Blue Team) será da ISH TECNOLOGIA, que irá analisar os logs e artefatos, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da ISH TECNOLOGIA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do MJSP.

Juntamente com o MJSP o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da ISH TECNOLOGIA, deverá definir a severidade/impacto do incidente. A severidade/impacto do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança (CSIRT – Blue Team) da ISH, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

Todo o processo de análise e resultados obtidos, serão documentados a todo tempo na ferramenta de ITSM, para que o MJSP acompanhe todos os passos para a solução do incidente.

Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente (Blue Team) da ISH TECNOLOGIA, definirá uma estratégia para a mitigação e contenção do ataque em questão.

Mitigado o incidente de segurança, no próximo passo a ISH TECNOLOGIA através do grupo de resposta a incidente de segurança (CSIRT – Blue Team), iniciará o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança (CSIRT – Blue Team). Tal análise será realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente cibernético em questão.

Caso seja necessário a reconstrução do ataque, este deve ser realizado pela ISH TECNOLOGIA em ambiente controlado, usando-se por exemplo de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da ISH TECNOLOGIA.

O grupo de resposta a incidente de segurança (CSIRT – Blue Team) da ISH TECNOLOGIA, deve documentar na ferramenta de ITSM, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

A ISH TECNOLOGIA comunicará a área de segurança do Ministério as informações sobre os incidentes e quais as ações foram ou estão sendo tomadas para sua solução.

O serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team será responsável por monitorar equipamentos e softwares do MJSP, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços;

A ISH TECNOLOGIA proverá serviços de resposta aos incidentes de segurança da informação diante dos eventos registrados no monitoramento;

Os serviços de monitoramento e resposta a incidentes de segurança poderão ser prestados por meio de Centro de Operações de Segurança da Informação.

A ISH TECNOLOGIA irá buscar inteligência de proteção contra-ataques cibernéticos e sendo responsável por:

Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

Criar, em colaboração com a MJSP, casos de uso (regras) que devem ser implementados na Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

Revisar periodicamente as regras da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério realizando as adaptações e evoluções necessárias;

Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério;

A ISH TECNOLOGIA atuará proativamente na antecipação e identificação de incidentes cibernéticos, antes mesmo do impacto nos serviços;

A ISH TECNOLOGIA reagirá aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do MJSP;

A ISH TECNOLOGIA atuará quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI.

A ISH TECNOLOGIA realizará e apresentar relatório de testes de vulnerabilidades de todo o ambiente tecnológico, conforme as práticas de Segurança da Informação;

Gerará e consolidar os relatórios analíticos de ataques e ou incidentes contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do MJSP, contendo: hosts encontrados, topologia de rede, serviços, vulnerabilidade descobertas, nível de risco por plataforma e por vulnerabilidade, atualização de ativos sob sua administração, atualização de softwares (aplicação de patches e fix), sistemas de proteção, para apresentação ao MJSP, constando as medidas tomadas e sugestões;

Apresentará relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos, emitindo relatórios executivos, operacionais e de conformidade a norma NIST Cybersecurity Framework, Version 1.1 ou mais recente;

Monitorará e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados etc.), propondo ações corretivas e de melhorias;

A ISH TECNOLOGIA irá, quando da inexistência de empresa responsável pela infraestrutura do MJSP ou, quando o risco de exploração for considerado alto e a empresa responsável pela infraestrutura não atuar de forma tempestiva, aplicar correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório “Teste de Invasão” a partir do final da “Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste” de forma subsidiária, após autorização da área de segurança do MJSP.

A ISH TECNOLOGIA irá organizar a alocação de turnos e de profissionais de sua equipe.

A ISH TECNOLOGIA será responsável por realizar os testes em todos os sistemas ou ativos informados neste Termo de Referência, assim como, nos que vierem a existir na infraestrutura do MJSP.

Eventos:

A participação em eventos de Segurança da Informação nacionais ou internacionais deverá ser uma prática adotada pelo prestador visando estar alinhado ao estado da arte em termos de segurança da informação, sendo sugerida a participação da CRS com a indicação do evento, período, local e custos, provendo à CRS todos os meios pelos quais possa pleitear internamente junto a DTIC a participação de sua equipe e, em caso de impossibilidade de participação da equipe da CRS, prover o repasse das informações obtidas no evento tão logo do regresso dos participantes.

A ISH TECNOLOGIA irá divulgar ao menos a cada 6 (seis) meses a listagem de eventos nacionais e internacionais de Segurança da Informação para que o Ministério possa programar a participação dos servidores da área de segurança da informação. Na listagem de eventos deverá constar o nome do evento, período, local e custos relacionados ao evento como material, inscrição e outros.

O MJSP, no curso da execução contratual, poderá demandar a ISH TECNOLOGIA em temas relacionados a Segurança da Informação e Comunicação, visando auxiliar o MJSP no desempenho de suas atividades tais como, mas não se limitando a estas: verificação de conformidades no ambiente, confecção de relatórios, elaboração de documentos ou pareceres, avaliação de vulnerabilidades em aplicativos a serem instalados, especificação de requisitos de segurança para contratação de ativos ou serviços, auxiliar/avaliar na implantação de frameworks de segurança.

2.1.3. Requisitos de Perfis e Experiência Profissional

Para que haja garantia de qualidade no serviço executado e modernização das metodologias de Gestão de Risco e Segurança da Informação, a ISH TECNOLOGIA irá manter profissionais qualificados nas áreas funcionais, que deverão ser gerenciados exclusivamente pelo representante técnico da empresa ISH TECNOLOGIA, de forma que o MJSP possa obter o menor tempo de resposta para quaisquer incidentes ocorridos no seu ambiente de Infraestrutura tecnológica, bem como alcançar a excelência no serviço de TI;

Esses recursos humanos irão conhecer o funcionamento dos negócios internos da DTIC e demais áreas do Ministério, bem com executar os procedimentos de acordo com as regras de segurança;



As equipes irão ser dimensionadas pela empresa ISH TECNOLOGIA de forma a atender as demandas de acordo com os níveis mínimos de serviço exigidos estabelecidos. Para tanto, salienta-se que essa responsabilidade de formação da equipe de profissionais é exclusiva da empresa ISH TECNOLOGIA;

É de responsabilidade da ISH TECNOLOGIA o cumprimento da legislação específica dos profissionais que prestarão o serviço à MJSP;

Os profissionais irão utilizar vestimenta compatível com a utilizada pelos servidores do MJSP e portar crachá de identificação durante toda a prestação de serviço, quando de atuação presencial nas dependências do MJSP;

A ISH TECNOLOGIA irá ser responsável por qualquer deslocamento dos profissionais relacionados a execução do presente contrato. O tempo de deslocamentos não poderão ser utilizado para justificar o descumprimento dos Níveis Mínimos de Serviço Exigidos;

Durante a execução dos serviços, a ISH TECNOLOGIA irá disponibilizar os profissionais com as qualificações especificadas neste Termo de Referência. As certificações estarão ativas/válidas. As competências descritas podem estar presentes em diversos profissionais, cabendo a ISH TECNOLOGIA manter o número adequado de prestadores para cada atividade, respeitando apenas o quantitativo mínimo, porém não se limitando a ele;

A ISH TECNOLOGIA em um prazo de 90 dias para se adequará aos requisitos exigidos de certificações de seus profissionais, prazo esse que se inicia a partir da data da reunião inicial após a assinatura contratual e o mesmo pode ser renovado uma única vez por mais 90 dias, desde que a ISH TECNOLOGIA apresente justificativa a MJSP;

Durante a vigência contratual e a qualquer tempo, os profissionais da ISH TECNOLOGIA serão avaliados pela MJSP, a qual poderá solicitar a substituição destes, caso não estejam correspondendo às necessidades e requisitos para cada perfil. Esta substituição deverá ocorrer em até 15 quinze dias, contados a partir da notificação por parte da MJSP;

Serão aceitos como documentos válidos para comprovação de qualificação técnica os documentos citados pela legislação trabalhista, tais como: Carteira de Trabalho e Previdência Social, Contrato de Trabalho, Recibo de Pagamento de Trabalhador Autônomo, Sócio, Diretor. Quando a descrição contida nestes documentos não for suficiente para a comprovação da experiência exigida, estes poderão ser complementados com atestado(s) ou declaração(ões), descrevendo as atividades realizadas pelo profissional, expedido(s) por pessoa jurídica de direito público ou privado;

Para a qualificação em conhecimentos exigidos para a execução dos serviços serão aceitos certificados de participação em cursos e/ou certificações emitidas por instituições certificadoras especializadas;

Todos os profissionais que compõem a equipe possuirão residência física e fixa em território nacional e prestarão os seus serviços em instalações sediadas no país;

Durante a execução deste serviço a ISH TECNOLOGIA irá disponibilizar os profissionais com as qualificações abaixo especificadas:

Formação: Nível Superior completo em uma das seguintes áreas: Análise de Sistemas, Ciência da Computação, Processamento de Dados, Sistemas de Informação, Informática, Engenharia da Computação, Segurança da Informação ou curso superior completo em qualquer área e especialização, com no mínimo 360 horas, na área de segurança da informação.

Serviço de Security Operations Center - SOC:

Certificações para a função de Analista(s) SOC:

AZ-500: Microsoft Azure Security Technologies (Microsoft) - Pelo menos um profissional

CompTIA Security+ (CompTIA) - Pelo menos um profissional;

Fortinet Network Security Expert 4 – NSE4 (Fortinet)- Pelo menos um profissional;

Certificação ITILv3 Foundation ou superior - Pelo menos um profissional.

Experiência profissional para a função de Analista(s) SOC:

Experiência mínima de 4 (quatro) anos em utilização de analisadores de protocolo para realização de troubleshooting em plataformas SIEM;

Experiência mínima de 2 (dois) anos em implantação, administração e gerência de centralizador de logs;

Experiência mínima de 2 (dois) anos em administração de sistemas operacionais Linux;

Experiência mínima de 2 (dois) anos em administração de sistemas operacionais Windows Server 2012 ou superior;

Experiência mínima de 2 (dois) anos em análise forense, como análise logs, correlacionamento de eventos, resposta a incidentes de segurança da informação (cibernética);

Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team:

Certificações para a função de Especialista(s) Blue Team:

AZ-500: Microsoft Azure Security Technologies (Microsoft)- Ao menos um profissional

Certified Information Systems Security Professional - CISSP (ISC²) ou Certified Cloud Security Professional - CCSP (ISC²) - Pelo menos um profissional;

CompTIA Cybersecurity Analyst - CySA+ (CompTIA) - Pelo menos um profissional;

Certified Ethical Hacker - CEH (EC-Council) - Pelo menos um profissional;

CERTIFIED NETWORK DEFENDER - CND (EC-Council) - Pelo menos um profissional;

Fortinet Network Security Expert 4 – NSE4 (Fortinet) - Pelo menos um profissional;

FortiWeb Specialist Exam (fortinet) - Pelo menos um profissional;

Certificação ITILv3 Foundation ou superior - Pelo menos um profissional.

Experiência profissional para a função de Especialista(s) Blue Team:

Experiência mínima de 8 (oito) anos em utilização de analisadores de protocolo para realização de troubleshooting em plataformas de SIEM;

Experiência mínima de 8 (oito) anos em implantação, administração e gerência de centralizador de logs;

Experiência mínima de 8 (oito) anos em administração de sistemas operacionais Linux e Windows Server 2012 ou superior;

Experiência mínima de 4 (quatro) anos em atividades de Tratamento e Resposta aos Incidentes Cibernéticos Blue Team;

Experiência mínima de 4 (quatro) anos em análise forense, como análise de logs, correlacionamento de eventos, resposta a incidentes de segurança da informação (cibernética);

2.1.4. Deveres e responsabilidades do MJSP

Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

Receber o objeto fornecido pela ISH TECNOLOGIA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

Aplicar à ISH TECNOLOGIA as sanções administrativas regulamentares e contratuais cabíveis;

Liquidar o empenho e efetuar o pagamento à ISH TECNOLOGIA, dentro dos prazos preestabelecidos em contrato;

Comunicar à ISH TECNOLOGIA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da ISH TECNOLOGIA, com base em pesquisas de mercado, quando aplicável; e



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

Exigir o cumprimento de todas as obrigações assumidas pela ISH TECNOLOGIA, de acordo com as cláusulas contratuais e os termos de sua proposta.

Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

Notificar a ISH TECNOLOGIA por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

Permitir acesso dos empregados da ISH TECNOLOGIA às suas dependências para a execução dos serviços.

Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante ou preposto da ISH TECNOLOGIA.

Disponibilizar as instalações com espaço físico, o mobiliário e as estações de trabalho necessárias à execução dos serviços nas dependências do Ministério.

2.1.5. Deveres e responsabilidades da ISH TECNOLOGIA que irá:

Indicar formalmente preposto apto a representá-lo junto à MJSP, que irá responder pela fiel execução do contrato;

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

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

Propiciar todos os meios necessários à fiscalização do contrato pela MJSP, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

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

Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

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

Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, se for o caso, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a MJSP autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à ISH TECNOLOGIA, o valor correspondente aos danos sofridos.

Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à MJSP.

Relatar à MJSP toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

Não permitir a utilização de qualquer trabalho do menor de dezoito anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

Auxiliar o MJSP na elaboração de políticas e procedimentos relacionados à gestão e uso dos serviços contratados, inclusive no que tange à implantação de medidas de racionalização e economia.

Ser responsável exclusivo por quaisquer acidentes na execução dos serviços contratados e pela destruição ou dano dos documentos por culpa ou dolo de seus agentes.

A ISH TECNOLOGIA garante que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets, devendo a ISH TECNOLOGIA se responsabilizar por quaisquer despesas relacionadas que ocorram.

Assinar Termo de Confidencialidade no qual fica a ISH TECNOLOGIA impedida de liberar informações do órgão para empresas terceiras.

Fica a ISH TECNOLOGIA proibida de utilizar de dados ou informações do órgão para propaganda ou uso secundário não-autorizado.

O MJSP irá manter direitos exclusivos sobre todas as informações e dados gerados durante o período contratado. Essa propriedade inclui qualquer cópia disponível, inclusive backups de segurança.

Informar prontamente ao MJSP sobre fatos e/ou situações relacionadas à prestação dos serviços contratados que representem risco ao êxito da contratação ou o cumprimento de prazos exigidos, além de responsabilizar-se pelo conteúdo e veracidade das informações prestadas - sob pena de incorrer em situações de dolo ou omissão.

Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à MJSP.

O MJSP possui "Direito ao Esquecimento", ou seja, fica a ISH TECNOLOGIA obrigada a eliminar completamente qualquer dado ou informação obtida do órgão sob sua custódia ao término do contrato.

A ISH TECNOLOGIA deve informar os dados de telefone celular dos responsáveis pela empresa, incluindo um número principal e um adicional, para casos de emergência em que a Administração precise contatar os responsáveis (Importante esclarecer que os contatos principais ainda serão os comerciais, e que tais números serão utilizados apenas para os casos de emergência).

Será de responsabilidade da ISH TECNOLOGIA fornecer a seus técnicos todas as ferramentas, softwares e instrumentos necessários para a execução dos serviços, bem como prover e se responsabilizar pela locomoção dos mesmos até o Órgão.

A ISH TECNOLOGIA irá substituir qualquer profissional durante o decorrer do contrato, desde que avise à MJSP do fato, e indique o substituto para esse profissional.

Estabelecer, em conformidade à Portaria MJSP nº 513, de 2020, normas gerais de integridade em até 3(três) meses após a assinatura do contrato, caso esse ultrapasse o valor previsto no inciso I ou II do Art. 1º da referida portaria;

A implantação ou a adequação do Programa de Integridade poderá ser comprovada por qualquer documento hábil a ser encaminhado à equipe de fiscalização do contrato, preferencialmente, em meio digital.

Orientar seus empregados alocados para a execução do contrato sobre as normas de integridade e a indispensabilidade de seu cumprimento;

Adotar práticas de governança e gestão capazes de identificar e mitigar desvios de conduta, irregularidades, fraudes e atos ilícitos, de acordo com as normas de integridade previstas na Lei nº 12.846, de 1º de agosto de 2013, e no Decreto nº 8.420, de 18 de março de 2015;

Relatar ao órgão MJSP, por escrito, qualquer descumprimento das normas de integridade praticado por agentes públicos com os quais mantenha contato em decorrência da execução do contrato;

Substituir com presteza qualquer profissional que tenha cometido desvios de conduta, irregularidades, fraudes e atos ilícitos, conforme observado e notificado pelo agente público competente;

Apresentar, no momento da celebração do contrato, Declaração de Inexistência de Vínculo Familiar, nos termos do art. 7º do Decreto nº 7.203, de 4 de junho de 2010, em que é assumido o compromisso de não utilizar, na execução do contrato, mão de obra que seja cônjuge, companheiro ou parente em linha reta ou

colateral, por consanguinidade ou afinidade, até o terceiro grau, de agente público que exerce cargo em comissão ou função de confiança no âmbito do Ministério da Justiça e Segurança Pública;

Apresentar à equipe de fiscalização do contrato, juntamente com o rol de documentos obrigatórios do empregado alocado para a execução do contrato, Termo de Ciência e Concordância, devidamente assinado pelo empregado, conforme modelo constante no anexo à Portaria MJSP nº 513, de 2020 e a este Projeto Básico;

Encaminhar à equipe de fiscalização do contrato, observados os prazos estabelecidos na alínea “a”, documentação que evidencie, em alinhamento com os parâmetros do Capítulo IV do Decreto nº 8.420, de 2015, a realização das seguintes ações e atividades:

- promoção e participação em reuniões, apresentações, palestras e quaisquer outros eventos de natureza semelhante que evidenciam o comprometimento da alta direção da empresa em temas relacionados à integridade;

- mapeamento dos riscos de integridade e estabelecimento de ações mitigadoras, revisadas periodicamente;

- canal de denúncia, aberto e amplamente divulgado, com garantia do devido sigilo ao denunciante;

- código de ética ou de conduta aplicável a todos os dirigentes, administradores e empregados, independente de cargo, emprego, posto ou função exercidos;

- treinamentos periódicos sobre o Programa de Integridade, que envolvam as vedações incidentes na relação público-privada;

- promoção de campanhas para divulgar os princípios e valores que regem a empresa ISH TECNOLOGIA e o serviço público, bem como outros temas sobre integridade e combate a desvios de conduta, fraudes, irregularidades e atos ilícitos;

- adoção de medidas disciplinares, em caso de violação do Programa de Integridade, e de procedimentos e determinações que assegurem a pronta interrupção da tentativa ou da prática de desvios de conduta, fraudes, irregularidades e atos ilícitos;

- monitoramento contínuo do Programa de Integridade, com objetivo de aperfeiçoar os mecanismos de prevenção de atos lesivos, bem como sua detecção e combate; e

- encaminhamento semestral de relatório da execução do Programa de Integridade à equipe de fiscalização do contrato; e

Cumprir e exigir que os empregados alocados para a execução do contrato nas repartições administrativas cumpram, no que couber, as regras estabelecidas pelos órgãos do Ministério da Justiça e Segurança Pública

A ISH TECNOLOGIA irá apresentar, para aprovação da MJSP, no prazo máximo de 15 dias corridos, contados a partir da assinatura do contrato, Plano de Implantação dos Serviços, contendo cronograma detalhado de atividades a serem executadas pela ISH TECNOLOGIA.

Plano de Implantação deve conter, no mínimo, as seguintes informações: cronograma detalhado ao nível de atividades a serem desenvolvidas para a implantação de todos os serviços previstos no Termo de Referência; identificação de ferramentas e modelos a serem utilizados; configurações a serem realizadas; impactos e riscos, além do pessoal envolvido na execução dos serviços.

A ISH TECNOLOGIA deverá detalhar e repassar, conforme orientação e interesse do Ministério, todo o conhecimento técnico utilizado na implementação dos serviços, sem prejuízo da devida atualização da base de conhecimento ao longo de toda a execução.

3. DA VIGÊNCIA DO CONTRATO

O contrato terá vigência de 24 (vinte e quatro) meses a contar de sua assinatura, podendo ser prorrogado nos termos da lei.

4. NÍVEIS MÍNIMOS DE SERVIÇO

ID	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Unidade	Meta Exigida	Glosas (sobre o valor mensal)
Serviço de Security Operations Center - SOC (Grupo 1 - Item 01)					
1	Mensal – Índice Monitoramento de Infraestrutura. (Falha ou incidente de segurança de algum serviço ou equipamento de infraestrutura de TIC que deveria estar sendo monitorado e que a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério não foi devidamente configurada para tal apuração.)	Total de sistemas, serviços e equipamento monitorado pela Plataforma / Total de sistemas, serviços e equipamentos em produção x 100%	%	=100%	- 0,5% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
2	Mensal – Índice de Plano de Comunicação. (Não cumpra o escopo ou os prazos especificados no Plano de Comunicação para serviços que apresentarem incidentes de segurança da informação)	Total de plano de comunicação entregue / Total de plano de comunicação cumprido o escopo e/ou prazo x 100%	%	=100%	- 0,5% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
3	Mensal – Índice de Incidentes cibernéticos detectados. (Incidente cibernético de algum serviço do Ministério ocorrido sem que a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério tenha detectado porque não foi devidamente configurada para tal detecção.)	Total de incidentes cibernético detectados pela Plataforma / Total de incidentes cibernético ocorridos x 100%	%	=100%	- 5% por cada falta constatada aplicado sob o valor mensal do item 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
4	Quantidade de Vulnerabilidade(s) não relatadas e posteriormente identificadas. Obs.: Ver item 7.3.3.12.6	Soma das quantidades de vulnerabilidades não relatadas e posteriormente identificadas	Qt	0	Quando da ocorrência de vulnerabilidades não identificadas a Contratada será glosada mensalmente conforme segue: - 1% por vulnerabilidade com severidade baixa, limitada a 48 ocorrências durante a vigência contratual. 9 2% por vulnerabilidade com severidade média, limitada a 24 ocorrências durante a vigência contratual. 10 3% por vulnerabilidade com severidade alta, limitada a 12 ocorrências durante a vigência contratual. 11 5% por vulnerabilidade com severidade crítica, limitada a 4 ocorrências durante a vigência contratual. Aplicado sob o valor mensal dos itens 01 e 02. Caso algum dos limites de ocorrências seja superado, a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento, ou optar pela aplicação de glosa máxima permitida. A aplicação da glosa máxima será efetuada no pagamento referente ao mês de identificação do descumprimento da exigência.
					Quando da ocorrência de ataques sofridos com sucesso a Contratada será glosada mensalmente conforme segue: - 10% por impacto ao negócio baixo por evento limitado a 3 ocorrências durante a vigência contratual. - 20% por impacto ao negócio médio por evento limitado a 2 ocorrências durante a vigência contratual. - 40% por impacto ao negócio alto por evento, limitados a 1 ocorrência durante a vigência contratual.

Matriz: Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360
Filial RJ: Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021
Filial MG: Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020
Filial DF: SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905
Filial SP: Rua Surubim, nº 577/5º andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050
Integrasy: Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364

5	Quantidade de Ataque(s) bem-sucedidos com sucesso. Obs.: Ver item 7.3.3.12.7	Soma das quantidades de ataques ocorridos com sucesso	Qt	0	Aplicado sob o valor mensal dos itens 01 e 02. Caso algum dos limites de ocorrências seja superado, a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento, ou aplicar pela glosa máxima permitida no mês de identificação do descumprimento da exigência, ou optar pela aplicação de glosa máxima permitida. A aplicação da glosa máxima será efetuada no pagamento referente ao mês de identificação do descumprimento da exigência.
6	Mensal - Índice de Disponibilidade do SOC. (Falha, degradação ou indisponibilidade de operação do SOC sediado nas instalações da CONTRATADA para a prestação dos serviços contratados)	Indisponibilidade de sistema/serviços monitorados. 100 x (Horas Totais no Período = Dias do Mês x Horas Dias - Horas de Manutenção Preventiva - Horas Indisponíveis causadas por Terceiros - Horas Indisponíveis no Mês) / (Horas Totais no Período = Dias do Mês x Horas Dias - Horas de Manutenção Preventiva - Horas Indisponíveis no Mês)	99,70% e/ou média de performance mensal auferida (será considerada a média histórica dos últimos 30 dias)	%	0,5% para cada décimo percentual ou fração menor que a meta definida por indicador até o limite de 98,70% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 10% da média mensal (será considerada a média histórica dos últimos 30 dias). 1% para cada décimo percentual ou fração menor que a meta definida por indicador entre os limites de 98,69% até 97,70% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 20% da média mensal (será considerada a média histórica dos últimos 30 dias). 1,5% para cada décimo percentual ou fração menor que a meta definida por indicador abaixo do limite de 97,69% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 30% da média mensal (será considerada a média histórica dos últimos 30 dias). Aplicado sob o valor mensal do item 01. Obs: Os cálculos se referem a todo o ambiente mantido, ou seja, uma ou mais aplicações/serviços monitorados, a fórmula de cálculo é única, tendo como o limite total em 30%. Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
Atendimento das Requisições e dos Incidentes (Grupo 1 - Itens 01 e 02)					
7	Mensal - Índice de abertura de chamados (incidente e ou requisição) de atendimento com tratamento iniciado em até 5 minutos.	Total de chamados recepcionados em até 5 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	- 0,1% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
8	Mensal - Índice de triagem de incidentes e ou requisições abertos em até 15 minutos.	Total de triagem de incidentes e ou requisições abertos em até 15 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	0,2% por impacto ao negocio Baixa 0,4% por impacto ao negocio Médias e Altas Aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
9	Mensal - Índice de investigação de incidentes e ou requisições abertos em até 30 minutos.	Total de investigado de incidentes e ou requisições abertos em até 30 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	0,3% por impacto ao negocio Baixa 0,5% por impacto ao negocio Média 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
10	Mensal - Índice de resposta a incidentes e ou requisições abertos em até 1 hora.	Total de resposta a incidentes e ou requisições abertos em até 1 hora do recebimento / Total de chamados recebidos x 100%	%	>=80%	0,3% por impacto ao negocio Baixa 0,5% por impacto ao negocio Média 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.

Matriz: Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360
Filial RJ: Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021
Filial MG: Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020
Filial DF: SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905
Filial SP: Rua Surubim, nº 577/5º andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050
Integrasys: Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364

11	Mensal - Índice de resposta a incidentes e ou requisições abertos em até 2 horas.	Total de resposta a incidentes e ou requisições abertos em até 2 horas do recebimento / Total de chamados recebidos x 100%	%	>=90%	0,3% por impacto ao negocio Baixa 0,5% por impacto ao negocio Média 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
12	Mensal – Índice recorrência de incidentes e ou requisições abertos (Reincidência de abertura de chamados por falta de atuação da Contratada)	Total de requisições e ou incidentes reabertos / Total de solicitações mês x 100%	%	<=1% do total de solicitações/mês	5% para quando for superior à meta definida até o limite de 2% dos incidentes; 10% acumulativo para quando for superior a 2,1% até o limite de 5% dos incidentes; 15% acumulativos para quando for superior a 5,1% até o limite de 8% dos incidentes. Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
13	Mensal - Índice de atendimento para demandas dentro das dependências físicas do MJSP em situações de ocorrências de incidentes e problemas graves, conforme item 6.1.4.5, dentro de 15 minutos	Total de atendimentos a demandas em situações de ocorrências de incidentes e problemas graves em até 15 minutos / Total de atendimentos a demanda em em situações de ocorrências de incidentes e problemas graves x 100%	%	<=1% do total de solicitações/mês	5% para quando for superior à meta definida até o limite de 2% dos incidentes; 10% acumulativo para quando for superior a 2,1% até o limite de 5% dos incidentes; 15% acumulativos para quando for superior a 5,1% até o limite de 8% dos incidentes. Aplicado sob o valor mensal dos itens 01 e 02

5. DECLARAÇÃO DE DISPONIBILIZAÇÃO DA CENTRAL DE ATENDIMENTO

Declaramos a disponibilização de “Central de Atendimento” 24x7 para abertura de chamados técnicos.

Declaramos ainda a disponibilização de SOC, conforme exigências do edital para atendimentos dos serviços solicitados.

Nome (Razão Social): ISH Tecnologia S/A

Meios para abertura de chamado técnico		
Tipo	Dados	Meio Preferencial
Telefone (0800 ou custo local em Brasília)	0800 726-8926	Sim
E-mail	snoc@ish.com.br	Sim
Endereço Web	https://snoc.ish.com.br	Sim

Matriz: Rua Judith Maria Tovar Varejão, nº 355 - Enseada do Suá - Vitória/ES - CEP 29050-360
Filial RJ: Av. Presidente Wilson, nº 231/9º andar - Centro - Rio de Janeiro/RJ - CEP 20030-021
Filial MG: Av. Getúlio Vargas, nº 887/Sala 401 - Funcionários - Belo Horizonte/MG - CEP 30112-020
Filial DF: SCN Quadra 01, Bloco F/Salas 102 a 104, Ed América Office Tower - Brasília/DF CEP 70711-905
Filial SP: Rua Surubim, nº 577/5º andar - Ed. Igarassu - Brooklin - São Paulo/SP CEP - 04571-050
Integrasys: Rua Alberto de Oliveira Santos, nº 42/Sala 1802, Edifício Pasteur - Centro, Vitória - ES - CEP: 29.010-364