Gobierno del Estado de Sinaloa
Secretaría de Administración y Finanzas
Subsecretaría de Administración

Convocatoria a la Licitación Pública Nacional Número GES 22/2024

Contratación de Licenciamiento de Software, para la solución de visibilidad, clasificación, evaluación de riesgo, perfilamiento, segmentación y control de activos en la red. Así mismo, como para los servicios de informática por la evaluación y validación contra ransomware "SEXi", solicitado por la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales.

A N E X O I
Especificaciones Técnicas

COORDINACIÓN DE DESARROLLO TECNOLÓGICO		
ANEXO		
1		ANEXO TÉCNICO PARA LA SOLICITUD SERVICIO INTEGRAL DE CIBERSEGURIDAD QUE BRINDE VISIBILIDAD, CLASIFICACIÓN, PERFILAMIENTO, EVALUACIÓN DE RIESGO, SEGMENTACIÓN Y CONTROL DE ACTIVOS EN LA RED, ASÍ COMO LAS PRUEBAS PARA IDENTIFICAR Y CORREGIR LAS BRECHAS EN CONTRA DEL RANSOMWARE "**. SEXi"** QUE PRESENTEN LAS DEPENDENCIAS Y ORGANISMOS DEL GOBIERNO DEL ESTADO DE SINALOA, QUE CONVOCA LA COORDINACIÓN GENERAL DE DESARROLLO TECNOLÓGICO Y PROYECTOS ESPECIALES, CONTARÁ CON LOS SIGUIENTES REQUERIMIENTOS: El presente estipula los requerimientos asociados a la solución integral de ciberseguridad para la visibilidad, segmentación y control de activos en la red, así como para la detección y corrección de brechas que presente el Gobierno del Estado de Sinaloa en contra del ransomware. SEXi. **1. OBJETIVOS:** 1. Incrementar la seguridad de las operaciones de la organización a través de la simulación del ataque de ransomware. SEXi que permita identificar y corregir las brechas actuales. 2. Incrementar la seguridad de las operaciones de la organización a través de la visibilidad, segmentación y control de activos interactuando en la red del Gobiernos del Estado de Sinaloa. 3. Adquirir un servicio que permita la detección de brechas y vulnerabilidades que puedan ser explotadas para materializar el ransomware. SEXi dentro de la organización. 4. Adquirir la tecnología necesaria que permita lograr visibilidad, clasificación, perfilamiento, evaluación de riesgo, segmentación y control de todos los activos identificados en la red. 5. El servicio adquirido debe integrarse con las capacidades de ciberseguridad ya adquiridas por la organización. 6. Reducir los tiempos de detección, clasificación, segmentación y control de los dispositivos que interactúan en la red. 7. Fortalecer el proceso de identificación y control de activos conectados a la red. 8. Asegurar los procesos críticos del negocio garantizando los accesos necesarios basados en roles. PRESTACIÓN DE SERVICIO PRINCIPAL: 1. Solución integral de ciberseguridad para garantizar la visibilidad, segmentación y control de activos en la red, actualizaciones de software y soporte técnico (escalamiento) del fabricante por el periodo de 12 meses, así como la detección y corrección de brechas que presente el Gobierno del Estado de Sinaloa en contra del ransomware. SEXi. 2. Ejecución de pruebas de simulación de amenazas para detectar y corregir las brechas de ciberseguridad encontradas que permitan la ejecución y afectación del ransomware. SEXi en el Gobierno del Estado de Sinaloa.

PRESTACIÓN DE SERVICIO COMPLEMENTARIA:

1. Servicio de mesa de ayuda y soporte técnico **local** 24 x 7.
2. Servicio de mantenimiento técnico preventivo **local**.
3. Mesa de servicios (llamadas y correos electrónicos ilimitados) 24 x 7
4. Asistencia en sitio (12 meses) con tiempo de respuesta no mayor a 4 hrs
5. Entrega de informes mensual (presencial)
6. Equipo de respuesta a incidentes en sitio
7. Consultoría y acompañamiento para las actividades de remediación en sitio
8. Transferencia de conocimientos de la tecnología (hasta 12 participantes)

** Todo el apoyo solicitado por Gobierno de Sinaloa tendrá que ser brindado en sitio

CONDICIONES GENERALES

Proporcionar, con el correspondiente respaldo del fabricante, los servicios que corresponden a la prestación principal. Se deben incluir los servicios de actualizaciones de software y soporte técnico, del fabricante, por el periodo de un (1) año, contabilizado a partir de la fecha indicada en el acta de inicio de servicio (que establece la conformidad de implementación del mismo).

Contar con autorización del fabricante o su representante, para comercializar la marca y brindar las suscripciones requeridas.

Presentar una relación descriptiva de los componentes proporcionados como parte del servicio, incluyendo sus códigos comerciales (en tanto sea aplicable).

El canal participante deberá presentar una carta emitida por el fabricante (relacionada con la presente licitación) que avale la capacidad del canal para revender, distribuir o proporcionar servicios profesionales de la solución.

2.- ANTECEDENTES:

Con fundamento en lo establecido en el Plan Estatal de Desarrollo 2022-2027 en su apartado Interacción Digital y Tecnología, en el cual se enfatiza a la Interacción Digital y al Uso de Tecnologías Innovadoras como elementos clave para generar grandes transformaciones, haciendo uso efectivo y racional de la tecnología y herramientas de gestión, resulta imperativo proteger mediante soluciones vanguardistas que para lograr control granular de todos los dispositivos interconectados e interactuando en la red.
Así mismo, la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales, atendiendo las atribuciones marcadas en su reglamento interior artículo 35, fracciones XXXI, XXXII, XXXIII y 45 fracciones V, VI, XIV y XV, en relación a la conducción hacia el correcto cumplimiento de los estándares de seguridad definidos; así como diseñar e implementar políticas, normas y procedimientos de seguridad de la información y contar con mecanismos de seguridad para la protección de los datos personales que obren en su poder las dependencias y organismos de la administración pública estatal.
Para llevar a cabo la solución mencionada, la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales requiere de servicios profesionales, un equipo y herramienta especializada y de desarrollo muy robusto, actualmente existe una estructura muy limitada que desarrolle los servicios tecnológicos necesarios para este tipo de soluciones requeridas. En consecuencia, resulta imperativo el poder contratar este tipo de servicios y que se realicen bajo la supervisión de la Coordinación de Desarrollo Tecnológico.

3.- DESCRIPCIÓN DE LOS REQUERIMIENTOS

La contratación de los servicios se hará por 12 meses y se compone de los siguientes elementos:

Partida 1	Servicio / Solución	Nombre del servicio
Solución de Visibilidad, Clasificación, Evaluación de Riesgo, Perfilamiento, Segmentación y Control de Activos en la Red.	1.1	Solución de Visibilidad, Clasificación, Evaluación de Riesgo, Perfilamiento, Segmentación y Control de Activos en la Red.
	1.2	Hardware en alta disponibilidad (appliance) que soporte el tráfico de la red de Gobierno de Sinaloa definido en la descripción general (1.1) del presente anexo
	1.3	Servicio de Implementación
	1.4	Servicios de Entrenamiento
Evaluación y validación contra ransomware. SEXi	1.5	El servicio profesional de simulación de la amenaza de Ransomware SEXi está diseñado para evaluar y validar la efectividad de los controles de seguridad implementados en la infraestructura tecnológica de la entidad gubernamental del estado de Sinaloa. Este servicio consiste en replicar de manera realista la entrega de múltiples variantes del ransomware SEXi. La simulación se llevará a cabo siguiendo los más altos estándares y mejores prácticas de la industria, garantizando una evaluación exhaustiva y precisa.

1.1 Cantidad: 1

SOLUCIÓN DE VISIBILIDAD, CLASIFICACIÓN, EVALUACIÓN DE RIESGO, PERFILAMIENTO, SEGMENTACIÓN Y CONTROL DE ACTIVOS EN LA RED

DESCRIPCIÓN GENERAL

La solución debe ofrecer visibilidad y clasificación y análisis de riesgo los dispositivos y ser una herramienta de control de acceso a todos los tipos de dispositivos conectados a la red. La solución debe ser capaz de integrarse con la infraestructura actual de la red, debe de presentar un mecanismo para la gestión de invitados, terceros y BYOD, utilizando un captive portal. La gestión de invitados debe ser manual o automática y debe presentar herramientas para que un sponsor pueda gestionar su acceso. La solución debe soportar 802.1x, pero este protocolo no debe ser necesario para implementarla.

La solución de Visibilidad, segmentación y control de activos en la red debe estar basada en **equipos físicos** para cubrir las siguientes necesidades:

- Capacidad para soportar hasta **20,000 dispositivos y hasta 400 switches o WLAN.**
- **Capacidad para monitar tráfico de hasta 10Gbps.**
- **Portal captivo que cuente con capacidad para soportar hasta 200 inicios de sesión (HTTP) por minuto.**
- Capacidad para integrarse con Switches y controladora de Wireless de las marcas descritas más adelante.
- Capacidad para soportar Autenticaciones 802.1X en caso de ser necesario pero que no sea una limitante para poder tener visibilidad y clasificación sobre los dispositivos administrados y NO administrados.
- Capacidades para trabajar con o sin agente.
- Capacidad de poder trabajar con diferentes tecnologías de conectividad líderes del mercado.
- Capacidad para poder trabajar en modo pre o post conexión.
- Capacidad para administrarse centralmente.

La solución de simulación de la amenaza Ransomware. SEXi y acompañamiento deberá considerar lo siguiente:

- Instalación de agente
- No debe causar daño o disrupción
- Validación de la efectividad de los controles perimetrales en contra de la amenaza Ransomware SEXi
- Deben contener y ser considerados en el ejercicio las **últimas vulnerabilidades publicadas**
- Como parte de los entregables se deberá adjuntar un anexo con el detalle de la amenaza y sus respectivas acciones simuladas, así como la mitigación (firmas) para la prevención de la amenaza Ransomware SEXi adecuada al control de seguridad implementado en Gobierno de Sinaloa (anexo del reporte técnico)
- Deberá correrse de manera remota
- El ejercicio **NO** se deberá extender más allá de 1 mes (considerando pruebas y entrega de resultados)
- La simulación de la amenaza no deberá tener un impacto negativo en el rendimiento y disponibilidad de la infraestructura de Gobierno de Sinaloa (no DoS)
- Se deberá simular la amenaza por HTTP y HTTPS
- Se deberá compartir indicadores de compromiso de la amenaza
- Se deberá proporcionar una descripción de las acciones de la amenaza simulada
- Identificación de áreas de mejora y provisión de recomendaciones para fortalecer la seguridad informática
- Presentación de resultados (estatus actual)
- Entrega de informes y resultados ejecutivos y técnicos que describan los hallazgos de la simulación y la efectividad de los controles de seguridad implementados en la infraestructura de Gobierno de Sinaloa
- La metodología que se utilice debe estar alineada a **mejores prácticas globales de ciberseguridad** o marcos de referencia **(MITRE ATT&CK y Unified Cyber Kill Chain).**

Gestión de la Solución *(Visibilidad, segmentación y control de activos en la red)*

- La administración de la solución debe de hacerse desde una consola única, no importando el número de localidades o dispositivos en la red
- La administración y configuración de la solución debe ser por medio de interfaz gráfica
- Toda la comunicación entre la consola y los appliances virtuales debe ser encriptada
- La consola debe presentar todos los dispositivos conectados y las características descubiertas de cada dispositivo. Las columnas de informaciones presentadas deben ser personalizables
- Se deben configurar las políticas a través de esta misma consola gráfica
- Los dispositivos que caigan en cada regla de la política deben presentarse en la misma consola
- Los dispositivos deben organizarse en grupos, basados en cualquier característica
- La consola debe presentar un inventario de dispositivos, organizándose por tipo, función, usuario y Sistema Operativo
- Las credenciales de acceso a la consola deben ser locales o integradas a las bases de usuarios como Active Directory
- La consola debe tener niveles de acceso distintos, personalizables por usuario o por Grupo del AD
- La consola debe presentar un Dashboard interactivo. En este dashboard debe tener la capacidad de presentar visiones de la siguiente información:
- Porcentaje de dispositivo por tipo
- Porcentaje de dispositivo por nivel de Compliance
- Número de dispositivos conectados a lo largo del tiempo
- Número de dispositivos en Wifi o cableado
- Porcentaje de usuarios Corporativos vc Invitados
- Mapeo de conexiones entre dispositivos
- Indicadores de compromiso por dispositivo

VISIBILIDAD

La solución debe proveer visibilidad en el instante en que un dispositivo se conecta a la red, sin agentes: proporcionar descubrimiento y visibilidad 100 % sin agentes de todos los dispositivos en el instante en que se conectan a la red. Con la capacidad de vincular un USUARIO a un DISPOSITIVO a una UBICACIÓN.

La solución debe ser capaz de identificar donde se conectó cada dispositivo a la red

- Controller y qué AP del Wifi
- SSID se usó para conexión
- Puerto de Switch
- Concentrador de VPN

La visibilidad deberá ser independiente del proveedor o solución de red alámbrica (Switches) o inalámbrica (Controladora Wireless), y conexiones de acceso remoto (VPN) con integración nativa y lista con al menos los siguientes proveedores de infraestructura de red que son los más comunes en el mercado:

- Cisco
- HPE
- Juniper
- Avaya
- Huawei
- Arista
- H3C
- Alcatel
- Brocade
- Dell Force10
- Extreme
- Hirschmann
- Dasan
- FortiSwitch

Para la visibilidad en ambientes inalámbricos a solución debe integrarse de manera nativa con al menos las siguientes plataformas de Wireless:

- Cisco
- Aruba
- Motorola
- Ruckus
- Xirrus
- AeroHive

La solución debe integrarse de manera nativa con las soluciones de nube pública y privada:

- Amazon AWS
- Microsoft Azure
- Vmware vCenter
- Cisco ACI

La solución debe integrarse ya sea con métodos agnósticos o integraciones basadas en API’s con al menos los siguientes entornos de VPN:

- Cisco
- Palo Alto Networks

- Fortinet
- Check Point
- F5
- Pulse Secure

La solución debe usar múltiples métodos para identificar la entrada de un nuevo dispositivo a la red:

- La solución debe ser capaz de leer el tráfico espejo, una o múltiples interfaces de la red para hallazgo de dispositivos conectados, análisis de tráfico, fingerprinting
- La solución debe ser capaz de: interpretar paquetes DHCP cuando visualizados por la interfaz espejo
- La solución debe de ser capaz de analizar el fingerprint de un dispositivo a través de DHCP
- La solución debe ser capaz de recibir tráfico DHCP enrutado a través de DHCP Relay
- Dirección del Dispositivo en la tabla del switch o default gateway
- Trap SNMP del controlador Wifi o del Switch donde se conectó el dispositivo
- Paquete 802.1x Auth, cuando la solución se está portando como servidor 802.1x
- Paquete 802.1x Accounting, incluso cuando la solución no se está portando como servidor 802.1x
- Flujos de Netflow
- La solución debe ser capaz de leer el tráfico NetFlow v9 o Sflow para hallazgo de dispositivos conectados, análisis de tráfico y fingerprinting
- Informado por medio de API, cuando el dispositivo sea una máquina en la nube AWS o Azure (Nube Pública)
- Vmware (ESXi & Vcenter)

Donde de manera mínima tenga capacidad de descubrir y dar visibilidad de:

- Inventario de todos los puertos y protocolos
- Mac Address
- IP Address
- Hostname
- Device banner
- OS Fingerprint
- Switch IP
- Switch Name
- Switch Port
- Switch interface config
- SSID
- Controller and AP
- PoE
- VLAN
- Newly discovered switches (CDP / LDP)
- Ability to see the number of devices on any switch port
- Netflow session data
- AWS EC2/Instance Profiling and Classification
- AWS IAM Profiling & Classification
- AWS VPC Profiling & Classification
- Azure Instance Profiling & Classification
- Azure Local Network Gateway Properties
- Azure VM Properties
- Azure Vnet Properties
- Data Center Visibility (Cisco ACI)
- Data Center Visibility (Cisco Meraki)

- Data center visibility (Vmware)
- Vmware vSphere Server

La solución debe integrarse de manera nativa con las siguientes bases de usuarios:

- OpenLDAP
- Active Directory
- RADIUS
- Base interna para gestión de visitantes

La solución debe construir un inventario de activos físicos o virtuales y proveer datos contextuales detallados sobre estos dispositivos, incluidos: tipo de dispositivo (tradicional, BYOD, IoT médico, IoT no médico, etc.) ubicación, identidad del usuario y función (empleado), contratista, paciente, invitado) y el nivel de cumplimiento para ese dispositivo en tiempo real.

La solución debe de ser capaz de dar visibilidad y monitorea las comunicaciones de la red en tiempo real y proporciona información contextual rica sobre los activos conectados, los protocolos y el contenido de las comunicaciones, así como poder mapear automáticamente los flujos de tráfico a una taxonomía lógica de usuarios, aplicaciones, servicios, funciones, ubicaciones, dispositivos y niveles de riesgo en toda la red empresarial

CLASIFICACIÓN

La solución debe ser capaz de utilizar la información derivada de la visibilidad de dispositivos para clasificarlos automáticamente a medida que se conectan a la red, por función y tipo, sistema operativo y versión y/o proveedor y modelo.

La solución deberá ser capaz de identificar el tipo de dispositivo por al menos estos métodos DHCP, NMAP, SPAN, Netflow, public/private cloud API's, device profile library.

La solución debe contar con proporcionar un servicio en tiempo real que permita: identificar, categorizar, y priorizar el riesgo en los dispositivos conectados en la red y detectados en la plataforma: IT, IoT, OT, tales como: Equipos de Cómputo, Servidores, Impresoras, Dispositivos Móviles, Equipos VoIP, equipos de Red), etc.

La solución debe permitir la evaluación y clasificación de los dispositivos de acuerdo con Indicadores de compromiso y los indicadores deben ser generados con base en el análisis de:

- Vulnerabilidades (CVE's)
- Puertos Abiertos
- Cumplimiento
- Criticidad del dispositivo en la organización
- Exposición a Internet
- Reputación de IP's

La clasificación mínima requerida son las siguientes:

- Los dispositivos conectados a la red deben clasificarse según su función
- Los dispositivos conectados a la red deben clasificarse según su SO
- Los dispositivos conectados a la red deben clasificarse según su Fabricante
- La clasificación debe hacerse con múltiples métodos. La solución debe soportar como mínimo los siguientes métodos:

- Fingerprint de DHCP
- Puertos TCP abiertos
- Cabecera HTTP vista al acceder al portal (captive portal)
- Cabecera HTTP vista en el tráfico espejo al acceder a cualquier sitio
- Tráfico de Autenticación generado por el dispositivo
- Otros tráficos generados por el dispositivo, vistos mediante NetFlow o tráfico espejo
- Banner de NMAP
- Datos obtenidos por el Switch
- Dominio NetBIOS
- Propiedades obtenidas de la nube privada o pública, como el SO de la VM
- Nombre configurado en el DNS
- Direcciones Ipv4 e Ipv6
- Presencia o ausencia de Agente de la Solución, instalado en el dispositivo
- Query SNMPv1, v2 y v3 al propio dispositivo

EVALUACIÓN

La solución debe de poder evaluar la postura de los dispositivos ya sean dispositivos corporativos, de invitados, dispositivos BYOD y dispositivos IoT sin la necesidad de instalar un agente en los dispositivos. Y con al menos los siguientes atributos:

- Asset ownership (Target/non-Target)
- Cloud instance posture
- Installed applications
- Logged in user
- Ability to read certificates
- Installed applications(s)
- Running applications(s)
- Open tcp/udp ports (implies scan of device)
- Antivirus Installed
- Antivirus Running
- Antivirus Update Date
- Device Interfaces
- Domain Member
- Expected Script Result (non-interactive)
- Expected Script Result (interactive)
- External Devices
- File Date
- File Exists
- File MD5 Signature
- File Size
- File Version
- File Version Comparison
- Hotfix Installed
- HTTP redirection to URL (if browser is opened at endpoint)
- Instant Messaging Installed
- Instant Messaging Running
- Intranet WSUS Server
- Is Behind NAT
- Kill Instant Messaging

- Kill Peer to Peer
- Kill Process on Windows
- Microsoft Applications Installed
- Microsoft Vulnerabilities
- Microsoft Vulnerabilities Fine-Tuned
- NetBIOS Domain
- NetBIOS Hostname
- NetBIOS Membership Type (domain or workgroup)
- Network Adapters
- Number of IP Addresses
- Peer to Peer Installed
- Peer to Peer Running
- Personal Firewall Active
- Registry Key Exists
- Registry Key Value
- Registry Value Exists
- Run Script on Window (non-interactive)
- Run Script on Window (interactive)
- Send Balloon Notification
- Set Registry Key
- Shared Folders
- Start Antivirus
- Start Windows Updates
- Update Antivirus
- Updates Installed - Reboot Required (property)
- User currently logged on
- Windows Processes Running
- Windows Security Center Antivirus Status
- Windows Services Installed
- Windows Services Running
- Windows Update Agent Installed
- Windows Version
- Windows Version CPE Format
- Windows Version Fine-Tuned

La solución debe soportar de manera nativa, como mínimo con las siguientes plataformas comerciales de antivirus. La solución debe dar identificar los siguientes antivirus instalados en los dispositivos:

- AhnLab
- Avast
- AVG
- Avira
- BitDefender
- E-Trust
- ClamAV
- Crowdstrike
- Comodo Antivirus
- eScan
- ESET Nod32
- F-Secure

- G Data
- Hauri
- Kaspersky
- KingSoft
- LightSpeed
- Mcafee
- Microsoft Security Essentials
- Microsoft Windows Defender
- Panda Antivirus
- Rising Antivirus
- Sophos Antivirus
- Symantec Antivirus
- Symantec Endpoint Protection
- Trend micro

La solución debe detectar si está instalado el software Peer-to-Peer. La solución debe soportar de manera nativa, como mínimo, los siguientes softwares:

- BearShare
- BitComet
- BitTorrent
- Deluge
- Kazaa
- Spotify
- Transmission
- UTorrent

La solución deberá ser capaz de descubrir si está instalado Personal Firewall. La solución debe soportar de manera nativa, como mínimo, los siguientes antivirus:

- Mcafee Endpoint Security
- Windows Personal Firewall
- Sophos Client Firewall
- Symantec Client Firewall
- Symantec Endpoint Protection
- Zone Labs ZoneAlarm

La solución deberá ser capaz de descubrir si está instalado el software de almacenamiento en la nube de al menos las siguientes marcas:

- Amazon Cloud Drive
- Apple iCloud Drive
- Box
- Dropbox

La solución debe ser capaz de identificar si el dispositivo este encriptado con al menos las siguientes soluciones de encripción:

- CheckPoint Full Disk Encryption
- BitLocker
- Symantec Endpoint Encryption

CONTROL

La solución debe ser capaz de tomar acciones de control o remediación de acuerdo con la evaluación de la postura

		de seguridad de los dispositivos a través de políticas granulares configuradas desde la consola. Flexibilidad de aplicación de control en el dispositivo en las fases de pre conexión o pos conexión Con base a los resultados del análisis de Riesgo y los indicadores de compromiso la solución debe permitir configurar acciones que permitan realizar segmentación, remediación y control de dichos dispositivos. Las integraciones de control pueden ser realizadas a través de SNMP y/o telnet y/o SSH, y/o 802.1x y/o puerto espejo o uso de API's, sin tener exclusiva dependencia de algún método para contar con una mejor cobertura de descubrimiento y visibilidad en ambos ambientes alámbrico e inalámbrica. Las medidas de control pueden ser de notificación, de control o restricción y remediación: • Permitir envío de alertas por correo al administrador de la plataforma • Permitir envío de alertas por correo dirigido a la mesa de ayuda • Permitir envío de alertas por correo dirigido al SOC • Permitir envío de alertas por correo dirigido al usuario • Permitir enviar notificaciones en pantalla al usuario • Permitir la redirección a un sitio web • Permitir enviar eventos de syslog o mensajes de CEF • Permitir cambio de VLAN del puerto de los switches, a través de SNMP y/o CLI • Permitir cambio de VLAN del puerto de los switches, a través de 802.1x en modo Proxy • Permitir cambio de VLAN del puerto de los switches, a través de 802.1x en modo Server • Permitir configuración de ACL en los switches, a través de SNMP y/o CLI • Permitir configuración de ACL en los switches, a través de 802.1x ACL • Permitir un shutdown del puerto de los switches, a través de SNMP y/o CLI • Permitir la restricción de conectividad del dispositivo a través de un Virtual Firewall implementado por el puerto de tráfico espejo, sin cambios en la configuración de ningún elemento de red • Permitir el redireccionamiento del acceso web de un dispositivo a un portal (Captive Portal) usando tráfico espejo • Permitir el redireccionamiento del acceso web de un dispositivo a un portal (Captive Portal) usando DNS • Permitir la desconexión de un usuario de Wireless, a través de SNMP y/o CLI • Permitir la desconexión de un usuario de Wireless, a través de 802.1x • Permitir el cambio en el perfil de conectividad de un usuario de Wireless, a través de SNMP y/o CLI • Permitir el cambio en el perfil de conectividad de un usuario de Wireless, a través de 802.1x • La solución debe gestionar la lista de control de acceso (ACL) sin la dependencia de 802.1x. • La solución debe ser capaz de interactuar con el tráfico, usando puerto espejo para redireccionar a un portal (captive portal) o bloqueando determinados tráficos. • En el ambiente inalámbrico la solución debe ser capaz de actuar como DNS Proxy, permitiendo responder pedidos de DNS, de usuarios de la red • Esta función se puede usar también para redireccionar usuarios a un portal (captive global) • La solución debe soportar el uso de 802.1x para autenticación de usuarios o dispositivos en la red, cuando sea necesario. • La solución debe soportar PEAP y EAP-TLS. • La solución debe soportar las extensiones de CoA (RFC 3576). • La solución debe funcionar en modo Proxy y también en modo Servidor. • Permitir el cambio en el perfil de conectividad de una Máquina Virtual en el VMWare ESX, a través del cambio del Port Group configurado en la VM • Permitir el cambio en el perfil de conectividad de una Máquina Virtual en el VMWare NSX, a través del cambio del Security Group configurado en la VM • Permitir el cambio en el perfil de conectividad de una Máquina Virtual en el VMWare NSX, a través del

cambio del Security TAG configurado en la VM

REMEDIACIÓN

Soporte Windows
La solución debe ser capaz de analizar y corregir estaciones Windows sin el uso de agente instalado en la máquina. Se deben soportar sin agente las funciones a continuación:

- Soportar como mínimo Windows 7, 8 y 10
- Soportar como mínimo Windows Server 2012, 2012R2 y 2016
- La solución debe determinar el nombre del usuario que hizo login en el dispositivo
- La solución debe cruzar esta información con el directorio activo (descritos en la sección de directorio activo) para obtener datos del usuario como nombre completo, email y grupos a los que pertenece.

Analizar si está instalado el antivirus. La solución debe soportar de manera nativa, como mínimo, los siguientes antivirus:

- AhnLab
- Avast
- AVG
- Avira
- BitDefender
- E-Trust
- ClamAV
- Crowdstrike
- Comodo Antivirus
- eScan
- ESET Nod32
- F-Secure
- G Data
- Hauri
- Kaspersky
- KingSoft
- LightSpeed
- Mcafee
- Microsoft Security Essentials
- Microsoft Windows Defender
- Panda Antivirus
- Rising Antivirus
- Sophos Antivirus
- Symantec Antivirus
- Symantec Endpoint Protection
- Trend micro

La solución debe ser capaz de analizar la fecha de actualización de cada antivirus mencionado arriba
La solución debe ser capaz de forzar que el dispositivo busque una actualización (corregir el problema) de cada antivirus mencionado arriba
La solución debe ser capaz de analizar si el Antivirus está en ejecución, para cada antivirus mencionado arriba
La solución debe ser capaz de forzar la ejecución de un antivirus detenido (corregir el problema) para cada antivirus mencionado arriba
Analizar si está instalado el software Peer-to-Peer. La solución debe soportar de manera nativa, como mínimo, los siguientes softwares:

- BearShare
- BitComet
- BitTorrent
- Deluge
- Kazaa
- Spotify
- Transmission
- uTorrent

La solución debe ser capaz de analizar si el Peer-to-Peer está en ejecución, para cada software mencionado arriba
La solución debe ser capaz de matar el proceso de Peer-to-peer ejecutándose (corregir el problema), para cada software mencionado arriba
Analizar si está instalado Personal Firewall. La solución debe soportar de manera nativa, como mínimo, los siguientes antivirus:

- Mcafee Endpoint Security
- Windows Personal Firewall
- Sophos Client Firewall
- Symantec Client Firewall
- Symantec Endpoint Protection
- Zone Labs ZoneAlarm

La solución debe ser capaz de analizar si el firewall está en ejecución, para cada software mencionado arriba
La solución debe ser capaz de iniciar la ejecución de un personal firewall (corregir el problema) para cada software mencionado arriba.

Analizar si está instalado el software de almacenamiento en la nube. La solución debe soportar de manera nativa, como mínimo, los siguientes softwares:

- Amazon Cloud Drive
- Apple iCloud Drive
- Box
- Dropbox

La solución debe ser capaz de analizar si el software está en ejecución, para cada software mencionado arriba
La solución debe ser capaz de matar el proceso de almacenamiento en la nube que está ejecutándose (corregir el problema), para cada software mencionado arriba.

Analizar si está instalado el software de almacenamiento en la nube. La solución debe soportar de manera nativa, como mínimo, los siguientes softwares:

- Check Point Full Disk Encryption
- BitLocker
- Symantec Endpoint Encryption

La solución debe ser capaz de analizar continuamente los procesos que están ejecutando en cada dispositivo.
La solución debe ser capaz de matar un proceso de manera nativa, configurando solamente el nombre del proceso.
La solución debe ser capaz de analizar continuamente los servicios que se están ejecutando en el SO.
La solución debe ser capaz de analizar los patches de windows que están faltando en el SO.

		La solución debe ser capaz de disparar un proceso de actualización de patches de forma automática (corrección.) Debe ser capaz de forzar a que busque directo en internet. Debe ser capaz de forzar a que busque un servidor WSUS configurado La solución debe ser capaz de leer cualquier clave de registro del SO La solución debe ser capaz de escribir claves de registro del SO La solución debe ser capaz de ejecutar scripts localmente en el SO del dispositivo que se está gestionando La solución debe ser capaz de identificar periféricos conectados a Windows y clasificarlos (impresora, iPhone, etc., por medio de USB) La solución debe ser capaz de identificar el dominio NetBIOS y la participación del dispositivo Windows en el dominio La solución debe ser capaz de identificar los compartidos de disco habilitados en el Windows del dispositivo que se está gestionando La solución debe ser capaz de analizar un archivo del SO, al comparar fecha, tamaño, versión y hash MD5. La solución debe determinar la versión exacta de Windows Todas las funciones del soporte a Windows también deben se posibles a través de agente Soporte Linux La solución debe ser capaz de analizar y corregir estaciones Linux sin el uso de agente instalado en la máquina. Se deben soportar sin agente las funciones a continuación: • Soportar como mínimo CentOS 5, 6 y 7 • Soportar como mínimo Debian 8 y 9 • Soportar como mínimo Fedora 18,19,20,21,22 y 23 • Soportar como mínimo Red Hat Enterprise Linux 5, 6 y 7 • Soportar como mínimo Red Hat Enterprise Linux Desktop 7 • Soportar como mínimo Ubuntu 12, 13, 14.0.4, 15, 16.0.4, 18.0.4 La solución debe ser capaz de identificar la versión exacta del SO instalado La solución debe ser capaz de analizar un archivo del SO, al comparar fecha, tamaño, versión y hash MD5 La solución debe ser capaz de determinar el hostname configurado en el SO La solución debe ser capaz de determinar el nombre de usuario cuyo login se hizo en el SO La solución debe ser capaz de analizar continuamente los procesos que están ejecutando en cada dispositivo La solución debe ser capaz de matar un proceso de manera nativa, configurando solamente el nombre del proceso. La solución debe ser capaz de ejecutar scripts localmente en el dispositivo que se está gestionando. Todas las funciones del soporte a Linux también deben ser posibles a través de agente Soporte MacOS. La solución debe ser capaz de analizar y corregir estaciones MacOS sin el uso de agente instalado en la máquina. Se deben soportar sin agente las funciones a continuación: Soportar como mínimo MacOS 10.12 hasta 12.X La solución debe ser capaz de identificar la versión exacta del SO instalado La solución debe ser capaz de analizar un archivo del SO, al comparar fecha, tamaño, versión y hash MD5 La solución debe ser capaz de determinar el hostname configurado en el SO La solución debe ser capaz de determinar el nombre de usuario cuyo login se hizo en el SO La solución debe ser capaz de analizar continuamente los procesos que están ejecutando en cada dispositivo. La solución debe ser capaz de matar un proceso de manera nativa, configurando solamente el nombre del proceso. La solución debe ser capaz de determinar todos los softwares instalados en el dispositivo que se está gestionando La solución debe ser capaz de analizar los patches del MacOS que están faltando en el SO. La solución debe ser capaz de disparar un proceso de actualización de patches de forma automática (corrección)

La solución debe ser capaz de ejecutar scripts localmente en el dispositivo que se está gestionando
Todas las funciones del soporte a MacOS también deben se posibles a través de agente
La solución debe ser capaz de analizar y de dispositivos IoT. Se deben soportar como mínimo las siguientes funciones:

- La solución debe clasificar el dispositivo IoT con respecto a su función en la red (impresora, cámara, trinquete, automatización, televisión, etc)
- La solución debe tener una base de dispositivos IoT preconfigurada con los dispositivos más comunes
- La solución debe actualizar esta base periódicamente y de forma independiente a la actualización del SO
- La solución debe permitir personalizar entradas, al categorizar nuevos dispositivos, diferentes o exclusivos del entorno siendo instalado.
- La solución debe permitir hacer query SNMP al dispositivo SNMP para determinar detalles
- Analizar el consumo de energía PoE del dispositivo y hacer monitoreo de cambios en el consumo
- Realizar intentos de login con usuarios conocidos por medio de telnet y ssh, para determinar la seguridad de los dispositivos IoT.
- La solución debe contener un listado de credenciales usadas comúnmente
- La solución debe permitir agregar un listado de credenciales típicas en el entorno

SEGMENTACIÓN

La solución debe ser capaz de proporcionar visibilidad de los flujos de comunicación por segmento de red, tipo de dispositivo, grupo o activo de interés, para fortalecer las estrategias de segmentación y Zero Trust del Gobierno de Sinaloa.

La solución deberá proporcionar capacidades de disminución de la superficie de ataque, limitando el radio de acción y mitigando los riesgos normativos y empresariales con una rápida aceleración de la estrategia de segmentación.

Deberá permitir configurar una matriz de visibilidad de acuerdo con las necesidades del cliente, para facilitar la identificación del flujo de comunicaciones.

La solución deberá ser capaz de diseñar, simular e implementar políticas que bloqueen el tráfico no deseado o limitar las comunicaciones de los dispositivos con grupos, segmentos o diferentes activos identificados, para garantizar la operación y disminuir la superficie de ataque.

AUTOMATIZACIÓN

La solución deberá ser capaz de intercambiar información y contexto de forma bidireccional con otras plataformas de ciberseguridad tales como:

EPP/EDR

- Carbon Black
- Crowdstrike
- Fireeye
- McAfee
- Symantec

VA

- Qualys
- Rapid7
- Tenable

		SIEM • IBM Qradar • Microfocus ArcSight • Splunk ATD • Checkpoint • Fireeye • Palo Alto Networks NGFW • Checkpoint • Fortinet • Palo Alto Networks PAM • CyberARK CMT • BIGFIX ITSM • Servicenow Advanced Compliance • OpenSCAP La plataforma debe soportar una arquitectura REST API para la comunicación con otras plataformas soportando acciones de visibilidad, control y orquestación. La plataforma debe utilizar un Plugin de intercambio bi-direccional de datos para integraciones a nivel de Bases de Datos. Capacidad para enviar atributos enriquecidos y personalizados de los dispositivos a través de syslog y mensaje CEF La solución debe ser capaz de interactuar con las soluciones de SIEM para: Disparar automáticamente acciones de corrección o control en un dispositivo específico, de acuerdo con una política configurada en la solución. La solución debe ser capaz de leer y consultar la herramienta de SIEM para obtener nuevas características de los dispositivos. Estas características deben poder hacer parte de las políticas de visibilidad, clasificación y Control La solución debe ser capaz de integrarse con Firewalls de nueva generación para crear el flujo automático de políticas en el firewall dependientes de acciones de control de la solución. La solución debe ser capaz de compartir información de configuración y contexto los dispositivos conectados a la red con herramientas de CMDB para mantener el repositorio de activos actualizado en tiempo real sin la necesidad de depender de 802.1x
	1.2	Cantidad: 1 **EQUIPAMIENTO (Servidor)** CPU avanzado que cumpla con las características que se mencionan a continuación: Hardware en alta disponibilidad (2 appliances) que cubra las características que se mencionan a continuación para dar soporte adecuado al tráfico de la red de Gobierno de Sinaloa:

		DESEMPEÑO - Soporte hasta 20,000 dispositivos - Soporte para hasta 400 switches o dispositivos WLAN - Autenticaciones a través de 802.1x de hasta 166 por segundo - Monitoreo de tráfico de hasta 10Gb/s - Portal captivo con capacidad de hasta 200 registros HTTP (logins) por minuto **EQUIPOS** - 1 unidad de rack - Interfaces de red 4x10/100/1000Mbps cobre - Interfaces de red SFP 4 (2x1G/10G dual rate) - Puerto serial DB9 (I/O Support) - Puerto USB 4-pin (USB 2.0) - Entrada de video (DB15) - DVD-ROM - 3 Discos duros (RAIS-1+HS) 600GB - Fuente de poder reduntante (2x 750W AC, 1’’-240VAC, 50 ~ 60Hz
	1.3	Cantidad: 1 **SERVICIO DE IMPLEMENTACIÓN** El Gobierno de Sinaloa para garantizar la correcta implementación de la solución requiere de servicios profesionales proporcionados por el Fabricante y acompañados del proveedor ganador. Los servicios deberán proporcionar como mínimo lo siguiente: Proporcionar una combinación óptima de servicios profesionales para poner en marcha la implementación de solución tecnológica e impulsar rápidamente el valor de esta en el entorno del Gobierno de Sinaloa a través de hitos predefinidos. Deberá proporcionar un arquitecto de soluciones que ayude a diseñar la mejor arquitectura para el Gobierno de Sinaloa y así mismo acompañarlo de un Customer Success Manager en todo momento. Deberá garantizar la implementación de todos los casos de uso que apliquen para el Gobierno de Sinaloa, evidenciando el correcto funcionamiento. Los servicios profesionales deberán entregar la evidencia del diseño de la arquitectura de la implementación. El proveedor favorecido deberá entregar una memoria técnica de la implementación de la solución. **PRUEBAS DE ASEGURAMIENTO DE CALIDAD** Pruebas de funcionalidad, para verificar que la solución hace exclusivamente lo que debe hacer, conforme a los requerimientos establecidos. Pruebas de desempeño, para evaluar la respuesta de la solución en niveles de saturación o de sometimiento a estrés. **ADMINISTRACIÓN, SEGUIMIENTO Y COMPROBACIÓN** • El proveedor deberá administrar y dará seguimiento a las solicitudes de mejora y mantenimiento de la solución.

		● El proveedor deberá entregar los reportes mensuales, mismos que se integrarán a la documentación comprobatoria y generará las facturas correspondientes del proveedor. ● **RESPONSABILIDAD DEL ADJUDICADO** El Adjudicado será el único responsable por la prestación en tiempo y forma de los servicios, ajustándose a las especificaciones, cantidades y condiciones requeridas por el presente Anexo Técnico, y en su caso a las indicaciones que al respecto reciba del Área Administradora del contrato y verificación de los Servicios.
	1.4	**SERVICIOS DE ENTRENAMIENTO** **Descripción General** Deberán de proporcionar un entrenamiento proporcionado directamente por el fabricante para 3 personas designadas por el Gobierno de Sinaloa, el entrenamiento deberá contar con curso virtual y voucher para realizar examen de certificación. **REQUISITOS PARA EL PROVEEDOR** ● El proveedor deberá contar con certificación vigente en Scrum Master. ● La oferta será fija e incondicionada y en moneda nacional para la vigencia del contrato ● El proveedor deberá contar con ingeniería propia (no subcontratada) que cumpla al menos con: ○ 2 ingenieros certificados como “Security Junior Penetration Tester” o similar ○ 1 ingeniero certificado como “Security Professional Penetration Tester” o similar ○ 1 ingeniero certificado en la plataforma de BAS (simulación de ataques) a utilizar ○ 1 ingeniero certificado como CISSP ○ 1 ingeniero certificado como CISM
	1.5	Cantidad: 1 **EVALUACIÓN Y VALIDACIÓN CONTRA RANSOMWARE. SEXI** El servicio profesional de simulación de la amenaza de Ransomware SEXi está diseñado para evaluar y validar la efectividad de los controles de seguridad implementados en la infraestructura tecnológica de la entidad gubernamental del estado de Sinaloa. Este servicio consiste en replicar de manera realista la entrega de múltiples variantes del ransomware SEXi. La simulación se llevará a cabo siguiendo los más altos estándares y mejores prácticas de la industria, garantizando una evaluación exhaustiva y precisa.

Gobierno del Estado de Sinaloa
Secretaría de Administración y Finanzas
Subsecretaría de Administración

Convocatoria a la Licitación Pública Nacional Número GES 22/2024

Contratación de Licenciamiento de Software, para la solución de visibilidad, clasificación, evaluación de riesgo, perfilamiento, segmentación y control de activos en la red. Así mismo, como para los servicios de informática por la evaluación y validación contra ransomware "SEXi", solicitado por la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales.

Anexo II
Propuesta Económica

Part	Sub. Part.	Cant.	Descripción	Costo Unitario	Importe
Contratación de Licenciamiento de Software					
1	1.1	1	SOLUCIÓN DE VISIBILIDAD, CLASIFICACIÓN, EVALUACIÓN DE RIESGO, PERFILAMIENTO, SEGMENTACIÓN Y CONTROL DE ACTIVOS EN LA RED.		
	1.2	1	EQUIPAMIENTO SERVIDOR // CPU AVANZADO		
	1.3	1	SERVICIO DE IMPLEMENTACIÓN		
	1.4	1	SERVICIOS DE ENTRENAMIENTO		
	1.5	1	EVALUACIÓN Y VALIDACIÓN CONTRA RANSOMWARE. SEXI		
			Subtotal		
			I.V.A		
			Total		

Gobierno del Estado de Sinaloa
Secretaría de Administración y Finanzas
Subsecretaría de Administración

Convocatoria a la Licitación Pública Nacional Número GES 22/2024

Contratación de Licenciamiento de Software, para la solución de visibilidad, clasificación, evaluación de riesgo, perfilamiento, segmentación y control de activos en la red. Así mismo, como para los servicios de informática por la evaluación y validación contra ransomware "SEXi", solicitado por la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales.

Anexo III

Escrito de Participación para la Junta de Aclaraciones

Lugar y Fecha:

Secretaría de Administración y Finanzas
del Gobierno del Estado de Sinaloa

At´n.- **Ing. Juan Carlos Vizcarra Estrada**
Subsecretario de Administración

Ref. Licitación Pública Nacional No. GES 22/2024

Por medio del presente, me permito manifestar el interés de la empresa (nombre de la empresa), de participar en la LICITACIÓN PUBLICA NACIONAL NÚMERO (NÚMERO), convocada por esa Subsecretaría a su digno cargo, en atención a lo anterior, me permito señalar la información legal de mí representada:

Registro Federal de Contribuyentes:	
Domicilio Fiscal (calle, numero, colonia):	Delegación o Municipio:
Código Postal:	Entidad Federativa:
Teléfono:	Fax: Correo Electrónico
Representante Legal:	Correo Electrónico:
No. Escritura Pública en la que consta su acta constitutiva: Datos de inscripción ante el Registro Público de la Propiedad y del Comercio:	
Nombre, número y lugar del Notario Público ante el cual se dio fé de la misma:	
Relación de Accionistas:	Apellido Paterno, Apellido Materno, Nombre (s)
Descripción del Objeto Social:	Transcribir en forma completa el objeto social, tal como aparece en su Acta Constitutiva tratándose de personas morales o Actividad Preponderante tratándose de personas físicas:
Reformas al Acta Constitutiva:	Si existen (en su caso manifestarlas, junto con datos registrales)
Nombre del apoderado o representante legal:	Apellido Paterno, Apellido Materno, Nombre (s)
Datos del documento mediante el cual acredita su personalidad y facultades No. Escritura Pública en la que consta su Acta Constitutiva:	Fecha:
Nombre, número y lugar del Notario Público ante el cual se protocolizo la misma:	

Lo anterior es con la finalidad de dar cumplimiento a las disposiciones legales que correspondan y a las Bases y Anexos de la Licitación Pública Nacional No. GES 22/2024.

Protesto lo necesario
(Firma autógrafa original)

Nota: para el licitante deberá incorporar textualmente los datos de los documentos legales que se solicitan en este documento sin utilizar abreviaturas principalmente en lo relativo a nombre de la persona física o razón social de la persona moral.

Gobierno del Estado de Sinaloa
Secretaría de Administración y Finanzas
Subsecretaría de Administración

Convocatoria a la Licitación Pública Nacional Número GES 22/2024.

Contratación de Licenciamiento de Software, para la solución de visibilidad, clasificación, evaluación de riesgo, perfilamiento, segmentación y control de activos en la red. Así mismo, como para los servicios de informática por la evaluación y validación contra ransomware "SEXi", solicitado por la Coordinación General de Desarrollo Tecnológico y Proyectos

Especiales Anexo III bis

Formato para la presentación de preguntas para la Junta de Aclaraciones.

Solicitudes de aclaración efectuadas por:

Nombre de la empresa:

(Las preguntas a las respuestas se agrupan preferentemente por tema o numeral de la convocatoria a la licitación para proceder a su respuesta):

Ejemplo:

A) Preguntas administrativas:

1.- Pregunta ----------? (Licitante)

Respuesta: ---------- (Convocante)

2.- ----------

B) Preguntas Técnicas:

1.- Pregunta ----------? (Licitante)

Respuesta: ---------- (Área Técnica)

2.- ----------

Nota: Se deberá utilizar tipo de letra Arial 10, no se deberán insertar tablas, ni viñetas, ni imágenes.

Gobierno del Estado de Sinaloa
Secretaría de Administración y Finanzas
Subsecretaría de Administración

Convocatoria a la Licitación Pública Nacional Número GES 22/2024.

Anexo IV
(Modelo de Contrato)

Contratación de Licenciamiento de Software, para la solución de visibilidad, clasificación, evaluación de riesgo, perfilamiento, segmentación y control de activos en la red. Así mismo, como para los servicios de informática por la evaluación y validación contra ransomware "SEXi", solicitado por la Coordinación General de Desarrollo Tecnológico y Proyectos Especiales.

Contrato para la adquisición de -----, que celebran por una parte **Gobierno del Estado de Sinaloa**, representado en este acto por la Lic. -------, Subsecretaria de Administración de la Secretaría de Administración y Finanzas, a quien en lo sucesivo se le denominará **"El Estado"** y por la otra parte la empresa: -------, representada por el C. ------, a la que en lo sucesivo se le denominará **"La Empresa"**, al tenor de las siguientes declaraciones y cláusulas:

D e c l a r a c i o n e s

I. "El Estado" , a través de su representante, declara:

I.1.Que el Estado de Sinaloa es una entidad federativa que forma parte integrante de la federación, conforme a lo dispuesto por los Artículos 43 de la Constitución Política de los Estados Unidos Mexicanos y 1º de la Constitución Política del Estado de Sinaloa; constituida como persona moral de acuerdo a las leyes relativas aplicables del Estado de Sinaloa.

I.2.Que es su representante legal y Subsecretaria de Administración, y cuenta con las facultades suficientes para suscribir el presente contrato otorgadas por el Poder Ejecutivo del Gobierno del Estado de Sinaloa, conforme al poder notarial consignado en Escritura Pública No. ----, del Volumen ----, de fecha -------, del protocolo a cargo del Notario Público Número ----, Licenciado ---------- de esta ciudad.

I.3.Que requiere de la adquisición de ---- para la (dependencia solicitante), cuya descripción se detalla en la Cláusula Primera de este Contrato, para lo cual se cuenta con los recursos presupuestales correspondientes.

I.4.Que en términos del Artículo 36, de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, se procedió a emitir la convocatoria correspondiente para llevar a cabo la Licitación Pública Nacional No. GES 22/2024, habiéndose emitido el dictamen correspondiente mediante el cual se adjudicó el presente contrato a favor de **"La Empresa"** signante.

I.5.La autorización de los recursos para la presente contratación se llevó a cabo mediante ------ con cargo a --------.

I.6.Señala como su domicilio el ubicado en Avenida Insurgentes s/n, Colonia Centro Sinaloa, C.P. 80129 en la ciudad de Culiacán, Sinaloa, mismo que se precisa para todos los fines y efectos legales de este contrato.

II. "La Empresa", a través de su representante, declara:

II.1 Que es una sociedad anónima debidamente constituida conforme a las leyes vigentes, según testimonio de Escritura Pública No. ---- de fecha -----, protocolizada por el Lic. ------, Notario Público No. ----- del Distrito Judicial de Culiacán, Sinaloa y registrada bajo (datos de inscripción registral y/o folio electrónico) del Registro Público de la Propiedad y del Comercio de la Ciudad ---- inscrita en el Registro Federal de Contribuyentes bajo el número --------.

II.2 Estar debidamente facultado para contratar y obligarse en los términos y alcances de este contrato, a nombre de su representada tal y como lo acredita con la Escritura Pública No. -----, Volumen ------, de fecha -----, del protocolo a cargo del Notario Público ------ en el Estado, Lic. -----, mismas facultades que a la fecha no le han sido revocadas ni limitadas en forma alguna.

II.3 Que su objeto social entre otros es la (se menciona la actividad de la empresa)

II.4 Que cuenta con la capacidad administrativa, técnica y financiera suficiente para cumplir con las obligaciones derivadas del presente contrato.

II.5 Que señala como domicilio de **"La Empresa"** el ubicado en calle ------- número -----, colonia ----, (nombre de la ciudad) mismo que se precisa para todos los fines y efectos legales de este contrato.

III. De las partes.

De conformidad con lo anterior, las partes manifiestan que se reconocen recíprocamente la personalidad con la que comparecen, por lo cual proceden a celebrar el presente contrato de acuerdo a las siguientes:

C l á u s u l a s

Primera.- Objeto:

Por medio del presente contrato, **"La Empresa"** vende y **"El Estado"** compra, en precio fijo, lo siguiente:

PART.	CANT.	DESCRIPCIÓN	PRECIO UNITARIO	IMPORTE
1				
2				
3				
		SUB-TOTAL		
		I.V.A.		
		TOTAL		

Los bienes antes referidos deberán cumplir con las características y especificaciones contenidas en el Anexo (1, 2 etc) el cual forma parte del presente contrato.

Segunda.- Monto del Contrato.

"El Estado" pagará a **"La Empresa"** como valor de operación total por la adquisición de los bienes objeto del presente contrato la cantidad de $------- (número y letra), incluyendo el Impuesto al Valor Agregado.

Tercera.- Forma de Pago.

"El Estado" pagará a **"La Empresa"** un anticipo del -----% del importe total del presente contrato y el resto a la entrega y aceptación de los bienes y/o equipos.

Pagos que se efectuaran en Moneda Nacional, previa entrega de las fianzas correspondientes y la factura fiscal que los amparen, debiendo acompañar para la procedencia del pago final, el Acta de Entrega Recepción que señala la Cláusula Cuarta de este instrumento.

Los pagos se efectuarán en la Caja General de la Secretaría de Administración y Finanzas ubicada en el primer piso de la Unidad Administrativa de Gobierno del Estado de Sinaloa en la ciudad de Culiacán, Sinaloa.

Cuarta.- Lugar y Plazo de entrega:

"La Empresa" se compromete a entregar a **"El Estado"**, los bienes y/o equipos objeto del presente contrato, en las oficinas de -------, ubicadas en calle -------, numero -----, colonia-------, ciudad ----,

levantándose al efecto el Acta de Entrega Recepción con la intervención de un representante del (dependencia solicitante) y un representante de **"La Empresa"**.

"La Empresa" se obliga a entregar los bienes y/o equipos contratados en un plazo de ---- días hábiles contados a partir de la entrega del anticipo dicho plazo no podrá ampliarse ni habrá condonación de sanciones cuando el retraso se deba a causas imputables a **"La Empresa".**

"La Empresa" se responsabiliza de que los bienes y/o equipos objeto de este contrato serán entregados en estado idóneo y dentro del plazo citado en el párrafo que antecede, en el entendido de que se liberará de dicha responsabilidad una vez emitida el Acta de Entrega Recepción antes citada.

Quinta.-Obligaciones de "La Empresa". Para el debido cumplimiento de este contrato, **"La Empresa"** se obliga a:

A) Cumplir en tiempo y forma con la entrega de los bienes y/o equipos objeto de este contrato, a satisfacción de **"El Estado"** y conforme a lo establecido dentro del clausulado de este instrumento jurídico y a la normatividad aplicable en la materia.

B) Entregar los bienes y/o equipos objeto de este contrato, con las características técnicas ofertadas pro **"La Empresa"** conforme al concurso que determinó su adjudicación.

C) No ceder total o parcialmente los derechos y obligaciones derivados de este instrumento jurídico a favor de persona alguna, con excepción de los derechos de cobro, en cuyo caso se deberá contar con el consentimiento de **"El Estado"**.

Sexta.- Fianza de anticipo y de cumplimiento de contrato.

Fianza del Anticipo.

La garantía del anticipo será por la totalidad del monto concedido y se constituirá mediante fianza otorgada por Institución de Fianzas debidamente autorizada a favor de la Secretaría de Administración y Finanzas, debiendo contener los siguientes requisitos:

- Indicación del porcentaje e importe total garantizado con número y letra.

- Referencia de que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato.

- La información correspondiente al número de contrato, su fecha de firma así como la especificación de las obligaciones garantizadas.

- El señalamiento de la denominación o nombre del proveedor o fiado, domicilio legal y fiscal, registro federal de contribuyentes.

- La condición de que la vigencia de la fianza será hasta su total amortización, mediante la entrega de los bienes o la devolución total o parcial, según sea el caso, de la cantidad que por concepto de anticipo recibe su fiado.

- La condición de que la fianza solo podrá ser cancelada cuando así lo autorice expresamente y por escrito Gobierno del Estado de Sinaloa.

- El señalamiento de que esta garantía estará vigente en los casos en que Gobierno del Estado de Sinaloa, en el contrato otorgue prórrogas o esperas al proveedor o fiado, para el cumplimiento de sus obligaciones, así como durante la substanciación de todos los recursos legales o juicios que se interpongan en relación con este contrato hasta que se pronuncie resolución definitiva por autoridad competente, salvo que las partes se otorguen el finiquito de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato principal o fuente de las obligaciones, o cualquier otra circunstancia.

- Señalar el domicilio de la afianzadora en esta localidad para oír y recibir notificaciones de esta dependencia.

- La Institución de Fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el Artículo 95 de la Ley Federal de Instituciones de Fianzas, para la efectividad de la presente garantía, procedimiento al que también se sujetará para el caso de cobro de intereses que prevé el Artículo 95 Bis del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida.

- Así mismo esta fianza cubre, defectos y vicios ocultos de los bienes y la calidad del servicio, así como cualquier otra responsabilidad en que hubiere incurrido el proveedor, en los términos señalados en la convocatoria de Licitación, en el contrato respectivo y el Código Civil Federal.

Las partes acuerdan que para la cancelación de esta fianza será requisito indispensable la aprobación mediante manifestación expresa y por escrito de **"El Estado".**

Fianza para el cumplimiento del contrato.

La garantía deberá constituirse por **"La Empresa"** mediante fianza expedida por una institución debidamente autorizada en los términos de la Ley Federal de instituciones de Fianzas, en Moneda Nacional (peso mexicano), por un importe del 10% (diez por ciento) del monto total del contrato sin considerar el I.V.A. a favor de la Secretaría de Administración y Finanzas del Gobierno del Estado de Sinaloa, y deberá contener los siguientes requisitos:

- Indicación del porcentaje e importe total garantizado con número y letra.

- Referencia de que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato.

- La información correspondiente al número de contrato, su fecha de firma, así como la especificación de las obligaciones garantizadas.

- El señalamiento de la denominación o nombre del proveedor o fiado.

- La condición de que la vigencia de la fianza deberá quedar abierta para permitir que cumpla con su objetivo de forma tal que no podrá establecerse o estipularse plazo alguno que limite su vigencia, lo cual no debe confundirse con el plazo para el cumplimiento de las obligaciones previstas en el contrato y actos administrativos.

- La condición de que la fianza solo podrá ser cancelada cuando así lo autorice expresamente y por escrito Gobierno del Estado de Sinaloa.

- El señalamiento de que esta garantía estará vigente en los casos en que Gobierno del Estado de Sinaloa, en el contrato otorgue prórrogas o esperas al proveedor o fiado, para el cumplimiento de sus obligaciones, así como durante la substanciación de todos los recursos legales o juicios que se interpongan en relación con este contrato hasta que se pronuncie resolución definitiva por autoridad competente salvo que las partes se otorguen el finiquito de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato principal o fuente de las obligaciones, o cualquier otra circunstancia.

- Señalar el domicilio de la afianzadora en esta localidad para oír y recibir notificaciones de esta dependencia.

- La Institución de Fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el Artículo 95 de la Ley Federal de Instituciones de Fianzas, para la efectividad de la presente garantía, procedimiento al que también se sujetará para el caso de cobro de intereses que prevé el artículo 95 Bis del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida.
- Así mismo esta fianza cubre defectos y vicios ocultos de los bienes y la calidad del servicio, así como cualquier otra responsabilidad en que hubiere incurrido el proveedor, en los términos señalados en la convocatoria de Licitación, en el contrato respectivo y el Código Civil Federal.

“La Empresa” se obliga a mantener esta fianza, hasta por trescientos sesenta y cinco días posteriores a la fecha de la firma del Acta de Entrega Recepción de los bienes y/o equipos de acuerdo a lo estipulado en la Cláusula Cuarta, acordando las partes que para su cancelación será requisito indispensable la aprobación mediante manifestación expresa y por escrito de **“El Estado”**.

Las garantías de anticipo y cumplimiento, junto con el comprobante que acredite el pago de las mismas a la afianzadora deberán presentarse dentro de los 10 (diez) días naturales siguientes a la firma del presente contrato en Avenida Insurgentes s/n entre las calles José Aguilar Barraza y 16 de Septiembre, Colonia Centro Sinaloa, C.P. 80129, Culiacán, Sinaloa.

Séptima.- Garantías de los equipos.

“La Empresa” garantiza los equipos materia del presente contrato, durante el periodo de un año, que contará a parir de la fecha de entrega del mismo, contra cualquier defecto de fabricación así como el de no cumplir con las especificaciones requeridas, mala calidad de los materiales, mano de obra, etc.

Si dentro del periodo de garantía se presenta algún defecto o cualquiera de las circunstancias anteriores, **“La Empresa”** queda obligada a sustituir los bienes y/o equipos defectuosos en un periodo no mayor a 20 (veinte) días naturales contados a partir de su notificación sin cargo adicional para **“El Estado”**.

“La Empresa” se obliga a responder de los defectos y vicios ocultos de los bienes y/o equipos, así como de cualquier otra responsabilidad en las que hubiera incurrido, en los términos señalados en este contrato y en la legislación vigente.

La forma de empaque y transporte que debe utilizar, serán los que **“La Empresa”** determine como idóneos, toda vez que la integridad de los bienes y/o equipos es su responsabilidad hasta el momento de la aceptación de los mismos, los costos que se originen por estos conceptos son por cuenta de **“La Empresa”**.
“La Empresa” deberá cubrir todos los seguros de transporte de conservación, etc, que requieran los bienes y/o equipos hasta el momento de la firma del acta señalada en la Cláusula Cuarta.

Octava.- Límite de responsabilidades.

En caso de incumplimiento de este contrato, la responsabilidad de **“La Empresa”**, independientemente de la forma de acción que se ejercite, consiste en:

- Que **“El Estado”** le haga efectiva la fianza entregada para garantizar el cumplimiento del presente contrato.

- Reintegrar a **“El Estado”** cabalmente los recursos económicos que le hayan sido entregados hasta el momento del incumplimiento de cualquiera de las cláusulas y condiciones del presente contrato.

El pago por el límite de responsabilidades referido, que se derive del incumplimiento de los términos y condiciones de este contrato, atribuibles a **“La Empresa”** será efectuado de inmediato a la notificación que **“El Estado”** le realice por escrito a **“La Empresa”**.

Independientemente de lo anterior, para los efectos dispuestos por el Artículo 83 Fracción III, de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, **“El Estado”** dará vista a la Secretaría de Transparencia y Rendición de Cuentas, de cualquier incumplimiento en que **“La Empresa”** hubiese incurrido.

Novena.- “La Empresa” será responsable absoluto de obtener las licencias autorizaciones y permisos necesarios para el cumplimiento del presente contrato y en los casos en que se infrinjan derechos de autor, patentes o marcas, **“El Estado”** queda liberado de cualquier responsabilidad en caso de que se someta a **“La Empresa”** a juicio o proceso por este concepto.

Décima.- Penas convencionales.

En el caso de que **"La Empresa"** se atrase en la entrega de lo bienes y/o equipos objeto del presente contrato, las partes pactan la aplicación de una pena convencional la cual será a partir del primer día de atraso consistente en el importe correspondiente al 0.116% (punto ciento dieciséis por ciento) del importe, en función de los bienes y/o equipos no entregados por cada día de retraso, tomando como fecha de entrega el día que se reciban en el lugar de entrega de los bienes y/o equipos contratados, el cual será deducido del importe total a pagar y no excederán del monto de la garantía de cumplimiento del contrato.

Para el efecto anterior **"El Estado"** en cumplimiento a lo establecido en el Artículo 85 de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles del Estado de Sinaloa, harán del conocimiento de la Secretaría de Transparencia y Rendición de Cuentas este hecho, acompañando los elementos con que se cuente, a fin de que resuelva lo procedente en relación a la sanción.

El pago de los bienes y/o servicios quedará condicionado, proporcionalmente al pago que **"La Empresa"** debe efectuar por concepto de penas convencionales por atraso, en el entendido de que en el supuesto de que sea rescindido el contrato, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía.

En caso de rescisión del presente contrato. La aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

Además de las sanciones anteriormente mencionadas, serán aplicables todas aquellas que correspondan al incumplimiento de las condiciones, cláusulas y obligaciones señaladas en el presente contrato.

Décima Primera.- Rescisión.

"El Estado" podrá rescindir administrativamente este contrato sin necesidad de declaración judicial, cuando **"La Empresa"** incurra en incumplimiento de las obligaciones derivadas de la cláusulas del presente contrato, conforme al procedimiento establecido en el Artículo 65 de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, que sustancialmente consiste en:

I.- Se iniciará a partir de que a **"La Empresa"** le sea comunicado por escrito el incumplimiento en que haya incurrido, para que en un término de cinco días hábiles exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes.

II.- Transcurrido el término a que se refiere la fracción anterior, **"El Estado"** contará con un plazo de quince días para resolver, considerando los argumentos y pruebas que hubiere hecho valer a **"La Empresa".**

III.- Rescindido el contrato se formulará el finiquito correspondiente a efecto de hacer constar los pagos que deba efectuar a **"El Estado"** por concepto de los bienes recibidos hasta el momento de la rescisión.

Una vez rescindido este contrato, no procederá el cobro de penalizaciones ni la contabilización de las mismas para hacer efectiva la garantía de cumplimiento, siempre que estas causas sean el motivo de la rescisión.

Cuando **"El Estado"** rescinda el presente contrato, sin perjuicio del ejercicio de las demás acciones que procedan, aplicará lo establecido en la Cláusula "Limites de responsabilidades"

Décima Segunda.- Reconocimiento contractual.

El presente contrato constituye el acuerdo entre las partes en relación con el objeto del mismo y deben de respetarse todas las condiciones contenidas en las bases y en la propuesta técnica y económica utilizadas en el concurso del cual se deriva este contrato, mismas que forman parte del presente.

Las partes manifiestan que en la celebración del presente contrato no ha habido error o vicio o lesión alguna que vicien el consentimiento.

Décima Tercera.- Sostenimiento.

Las partes se obligan a sujetarse estrictamente para el cumplimiento del presente contrato a todas y cada una de las cláusulas del mismo, así como a los términos, lineamientos, procedimientos y requisitos que establecen, la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, de sus supletorios y demás que le sean aplicables.

Décima Cuarta.- Jurisdicción.

Para el cumplimiento del presente contrato, así como para todo aquello que no esté estipulado en el mismo, las partes acuerdan primariamente someterse al procedimiento de conciliación establecido en los Artículos 101, 102 y 103 de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, o bien al procedimiento para resolución de controversias y para efectos de interpretación y cumplimiento se someterán a la jurisdicción y competencia del Tribunal de lo Contencioso Administrativo del Estado de Sinaloa en los términos del Artículo 104 de la mencionada Ley por ende, **"La Empresa"** renuncia al fuero, competencia y jurisdicción que pudiera corresponderle por razones de su domicilio presente, futuro o cualquier otra causa.

Décima Quinta.- Administración, verificación, supervisión y aceptación de los bienes.

La dependencia solicitante dará seguimiento y verificará el cumplimiento de los derechos y obligaciones establecidos en este instrumento.

Los bienes se tendrán por recibidos previa revisión de **la dependencia solicitante**, la cual consistirá en la verificación del cumplimiento de las especificaciones establecidas y en su caso en los anexos respectivos, así como las contenidas en la propuesta técnica.

La dependencia solicitante rechazará los bienes o servicios que no cumplan las especificaciones establecidas en este contrato y en sus anexos, obligándose **"LA EMPRESA"** en este supuesto, a entregarlos nuevamente bajo su responsabilidad y sin costo adicional para **"EL ESTADO",** sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

Leído que fue el presente contrato y enteradas las partes de su contenido y alcance legal, lo firman en la ciudad de Culiacán, Sinaloa, el día ------- de 2024.

POR "EL ESTADO"	POR "LA EMPRESA"
_____	_____

T E S T I G O S

_____	_____