



## ANEXO A

### ESPECIFICACIONES TÉCNICAS DETALLADAS, SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA

PARTIDA	DESCRIPCIÓN GENERAL	UNIDAD DE MEDIDA	CANTIDAD
ÚNICA	SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD AUTÓNOMA DE SINALOA (UAS)	SERVICIOS	1

GLOSARIO DE TÉRMINOS TÉCNICOS	DESCRIPCIÓN GENERAL
BALANCEADOR	<b>SOLUCIÓN</b> de propósito para optimizar y mejorar los tiempos de respuesta de las aplicaciones mediante la distribución de cargas.
CUADRANTE DE GARTNER	Término utilizado para demostrar que la infraestructura propuesta por un <b>LICITANTE</b> ha sido analizada de manera objetiva y bajo un protocolo de pruebas por una empresa tercera que se dedica a evaluar tecnologías, misma que obtiene una valoración en uno de los 4 cuadrantes (De Nicho, Visionarios, Desafiantes y Lideres) y está se presenta bajo un reporte.
DNS	<b>SOLUCIÓN</b> de nombres de dominio.
FILTRADO DE CONTENIDO	<b>SOLUCIÓN</b> de monitoreo y protección de navegación segura a internet, utilizada por el personal de una empresa, entidad gubernamental, instituto escolar o <b>UNIVERSIDAD</b> .
FIREWALL	<b>SOLUCIÓN</b> de propósito para el control de acceso a la red (trust & Untrust).
IPS	<b>SOLUCIÓN</b> de protección de intrusos, por sus siglas en inglés Intructions Protection Systems.
NGFW	Next Generation Firewall, También conocidos como Firewall de nueva generación
SOC	Security Operation Center, que en su traducción simple es un centro de operaciones en seguridad.
SOLUCIÓN	Servicios administrados de seguridad informática.
SSL	Término para identificar un certificado cifrado
THROUGHPUT	Es la tasa de transferencia efectiva, se utiliza para definir el rendimiento.
TRUST	Término para identificar zona de confianza
UNTRUST	Término para identificar zona de desconfianza, utilizada comúnmente para referirse a zonas desde internet.
VPN	Virtual Private Network, comúnmente conocido como Red Privada Virtual y se utiliza para conexiones remotas
WAF	Firewall de aplicaciones web.
WAN	Wide Área Network, conocida como una Red de Área Amplia.



---

## REQUERIMIENTOS

LOS **SERVICIOS** REQUERIDOS Y QUE DEBERÁN SER PARTE DE LA **SOLUCIÓN** PROPUESTA POR PARTE DEL PROVEEDOR DEBERÁ INCLUIR AL MENOS LOS SIGUIENTES **SERVICIOS**:

- **HABILITACIÓN DE LOS SERVICIOS DE SEGURIDAD**

Son los **SERVICIOS** necesarios de seguridad perimetral (Firewalls, IPS, Filtrado Web, Firewall de Aplicaciones web, **SERVICIOS** de balanceo y DNS.), que se requiere proporcionar e instalar en sitio.

- **SERVICIOS SEGURIDAD**

Son los **SERVICIOS** necesarios que se requiere su implementación, configuración y puesta a punto a cargo del proveedor ganador (Firewalls, IPS, Filtrado Web, Firewall de Aplicaciones web, servicios de balanceo y DNS.); con respecto a los insumos de energía eléctrica, de servicio de red, espacio físico en rack, conectores ó convertidores propios de infraestructura de acceso de otros dispositivos (SW), serán provistas por la UNIVERSIDAD al momento de las implementaciones.

- **SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)**

El proveedor de los **SERVICIOS** debe contar con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en territorio nacional, el cual deberá contar con los certificados ISO9001, SO27001, ISO22301 e ISO20000, mismos que podrán ser acreditados presentando copia de los certificados.

El objetivo de este centro debe de ser la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad. La gestión del centro de operaciones de seguridad (SOC) por sus siglas en inglés (análisis de bloqueos de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad funcionamiento 7x24x365, etc.).

A la finalización de la vigencia del contrato, el proveedor de los **SERVICIOS** transferirá a nombre de la UNIVERSIDAD AUTONOMA DE SINALOA (UAS) toda la Infraestructura considerada para la prestación de los servicios, por lo que deberá realizar todas las gestiones para las sesiones correspondientes.



## 1 Especificaciones técnicas

### 2 **SERVICIOS DE SEGURIDAD**

Son los **SERVICIOS** necesarios de seguridad perimetral (Firewalls, IPS, Filtrado Web, Firewall de Aplicaciones web), **SERVICIOS** de balanceo y DNS, que se requiere proporcionar en la **UNIVERSIDAD**.

### 3 **SERVICIOS de Firewall**

#### **Descripción de los SERVICIOS:**

La **UAS** requiere de la seguridad y protección de control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo, el **LICITANTE** deberá presentar el reporte indicando que la **SOLUCIÓN** propuesta se encuentra en los cuadrantes mágicos de gartner 2021.

El **LICITANTE** deberá cumplir con las siguientes especificaciones funcionales mínimas:

#### **Detalles de los SERVICIOS:**

El **LICITANTE** deberá brindar el presente **SERVICIO** conforme lo siguiente:

- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.
- Control de ruta WAN inteligente con la capacidad de tráfico directo entre enlaces WAN basados en 3000 aplicaciones y usuarios/grupos de usuarios.
- La arquitectura propuesta por el **LICITANTE** deberá estar basada en appliance físicos con Integración y arquitectura de hardware patentada.
- La infraestructura a emplear para la prestación de los **SERVICIOS** por parte del **LICITANTE**, deberá ser de última generación y de uso exclusivo para las necesidades de la **UNIVERSIDAD**, por lo cual el **LICITANTE** deberá acreditar dentro de su propuesta técnica, mediante carta bajo protesta de decir verdad del fabricante, donde manifieste lo anterior e indique que la infraestructura proporcionada es totalmente nueva.

#### **LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ.**

- Incluir un sistema operativo desarrollado por el mismo fabricante.
- Soportar inspección SSL.
- Identificar y bloquear amenazas ocultas dentro del tráfico cifrado sin afectar el rendimiento.
- Realizar la gestión de políticas con opciones únicas de vista de sección o global
- Soportar modos basados en políticas y basados en políticas de NGFW.
- Soportar políticas de IPv4.
- Brindar visibilidad de actividades de seguridad, redes, dispositivos y usuarios
- Brindar estadísticas e información del sistema sobre el dispositivo de estructura conectado
- Soportar el protocolo SNMP v3



- Incluir las siguientes funcionalidades de seguridad:
  - Firewall
  - IPS
  - Filtrado web
  - VPN
- Dar soporte las siguientes funcionalidades de ruteo:
  - Enrutamiento estático y de políticas
  - Ruteo dinámico
  - Deberán soportar NAT estática y dinámica
- Cumplir las siguientes especificaciones mínimas y deberán estar distribuidos en los siguientes sitios:
  - **Sitios Central Rafael Buelna y Sitio Culiacán**
    - Equipos Firewall de siguiente generación en HA
    - Throughput de Firewall: 36 Gbps
    - Throughput de NGFW: 9.5 Gbps
    - Throughput de Protección de amenazas: 7 Gbps
    - Latencia de firewall: 1.54  $\mu$ s
    - Nuevas sesiones por segundo: 450,000
    - Sesiones concurrentes: 8 Millones
    - Políticas de Firewall: 10,000
    - Interfaces a cobre RJ45 a 1 Gbps: 8
    - Doble fuente redundante
  - **Sitio Mazatlán**
    - Equipos Firewall de siguiente generación
    - Throughput de Firewall: 32 Gbps
    - Throughput de NGFW: 6 Gbps
    - Throughput de Protección de amenazas: 5 Gbps
    - Latencia de firewall: 2.14  $\mu$ s
    - Nuevas sesiones por segundo: 450,000
    - Sesiones concurrentes: 4 Millones
    - Políticas de Firewall: 10,000
    - Interfaces a cobre RJ45 a 1 Gbps: 16
    - Doble fuente redundante
  - **Sitio Guasave, sitio Guamúchil y sitio Mochis**
    - Equipos Firewall de siguiente generación por sitio
    - Throughput de Firewall: 20 Gbps
    - Throughput de NGFW: 1.6 Gbps
    - Throughput de Protección de amenazas: 1 Gbps
    - Latencia de firewall: 4.97  $\mu$ s

- Nuevas sesiones por segundo: 56,000
- Sesiones concurrentes: 1.5 Millones
- Políticas de Firewall: 10,000
- Interfaces a cobre RJ45 a 1 Gbps: 12
- Doble fuente redundante

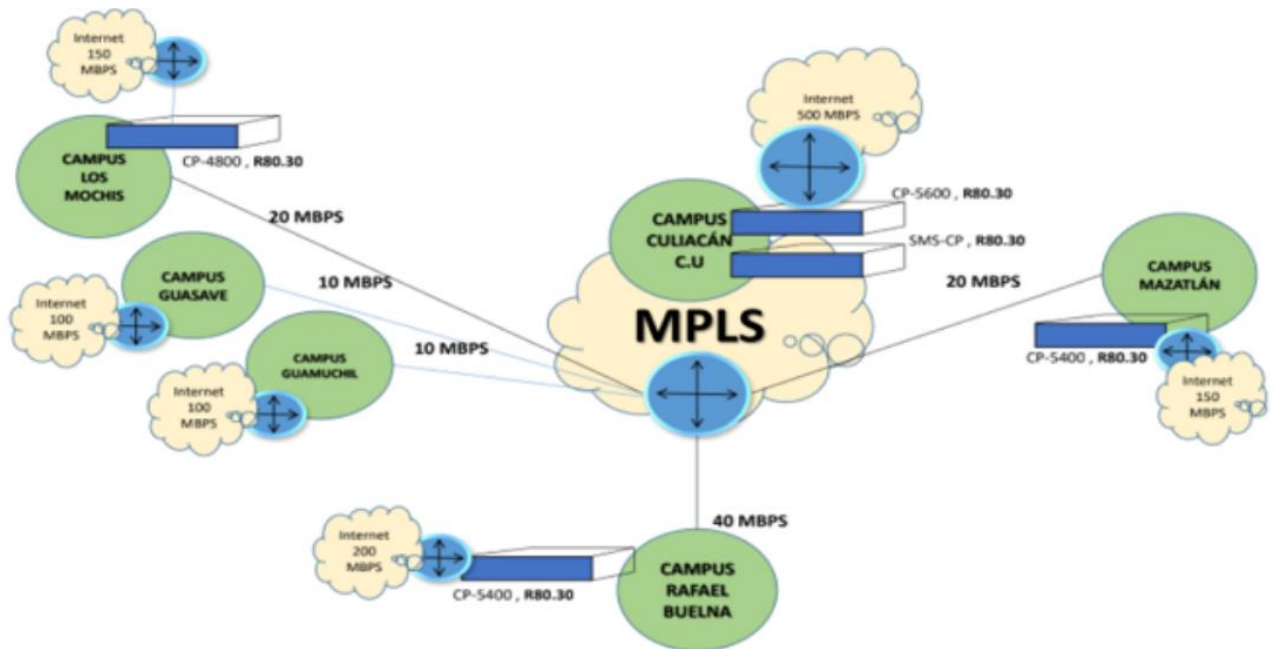


Diagrama 1

- Contar con una consola de administración centralizada on-premise para la gestión centralizada de los equipos firewalls.
- Tener consolas que proporcionen visibilidad, acceso y administración de los dispositivos Firewalls.
- Soportar las siguientes especificaciones técnicas:
  - Soportar los Equipos Firewalls de siguiente generación descritos en este anexo técnico.
  - Soportar configuración RAID1.
  - Contar con al menos 4 interfaces a cobre Rj45
  - Almacenamiento interno.

#### 4 SERVICIOS de Prevención de Intrusos (IPS)

##### Descripción de los SERVICIOS:

La **UNIVERSIDAD** requiere de los **SERVICIOS** de protección perimetral basado en firmas y que identifique vulnerabilidades, para contener los intentos de obtener acceso a los recursos o **SERVICIOS** publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información.



**Detalles de los SERVICIOS:**

- Habilitar los **SERVICIOS** de prevención de intrusos en la propia infraestructura de Firewall de nueva generación.
- Definir en conjunto con la **UNIVERSIDAD** la estrategia de habilitación de los nuevos **SERVICIOS** de infraestructura de prevención de intrusos (IPS por sus siglas en inglés) en la arquitectura de seguridad.

## 5 **SERVICIOS de Web**

**Descripción de los SERVICIOS:**

La **UNIVERSIDAD** requiere de los **SERVICIOS** de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización de los **SERVICIOS** de acceso a Internet, en función de roles y/o perfiles.

**Detalles de los SERVICIOS:**

- Habilitar los **SERVICIOS** de filtrado de contenido web en la propia infraestructura de Firewall de nueva generación.
- Habilitar las políticas para Filtrado de Contenido Web en la arquitectura de seguridad y de acceso perimetral.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que la **UNIVERSIDAD** genere.
- Monitorear todos los eventos registrados en la **SOLUCIÓN**, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el **SERVICIOS**.

## 6 **SERVICIOS de Firewall de Aplicaciones Web (WAF)**

**Descripción de los SERVICIOS:**

El proveedor deberá brindar una **SOLUCIÓN** de seguridad de aplicaciones web on-premise que permite proteger las aplicaciones Web alojadas en el sitio central y Culiacán de la **UNIVERSIDAD**, dicha **SOLUCIÓN** deberá ser de propósito específico tipo appliance. La **SOLUCIÓN** de WAF brindará las siguientes funcionalidades mínimas:

**Detalles de los SERVICIOS:**

**LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ**

- Soportar RESTful API para gestión de la configuración
- Ser capaz de enviar archivos para **SOLUCIÓN** de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo
- Contar con Aprendizaje automático (Machine learning) para detectar y bloquear amenazas y minimiza los falsos positivos.
- Realizar mitigación avanzada de Bots que permita proteger los activos web sin imponer ficciones a los usuarios legítimos.
- Proteger contra los siguientes ataques:



- Top 10 de OWASP.
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Tener integración con al menos las siguientes herramientas de vulnerabilidades:
  - IBM AppScan
  - Acunetix
  - HP WebInspect
  - Qualys
- Soportar los siguientes métodos de deployment:
  - Proxy Reverso
  - WCCP
  - Proxy transparente
  - En línea transparente
  - Fuera de línea
- Tener integración con los equipos Firewall de próxima generación.
- Soportar métodos de autenticación de al menos:
  - LDAP, RADIUS y SAML
  - Doble factor de autenticación
  - SSO
- Contar con las siguientes especificaciones técnicas:
  - El equipo deberá estar configurado en un esquema de alta disponibilidad activo/pasivo
  - Soportar un Throughput de 750 Mbps
  - Tener una Latencia de <5ms
  - Almacenamiento interno de 480 GB SSD
  - Contar con al menos 4 interfaces a cobre RJ45
  - Agregar fuente redundante (Opcional)

## 7 **SERVICIOS de Balanceo**

### **Descripción de los SERVICIOS:**

El proveedor deberá brindar una **SOLUCIÓN** balanceo local on-premise en un esquema de alta disponibilidad que permita la optimización Ochenta (80) aplicaciones y mejorar el tiempo de respuesta. Dicha **SOLUCIÓN** se requiere en el sitio central de la **UNIVERSIDAD** y deberá ser de propósito específico tipo Appliance.

### **Detalles de los SERVICIOS:**

#### **LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ**

- Soportar desplegar Global Load Balancer (GLB) detrás de dispositivos NAT
- Soportar Global Server Load Balancer (GSLB) sin necesidad de licenciamiento adicional



- Poseer una herramienta que permita ejecutar escaneo de vulnerabilidad a los servidores web balanceados y poder así mejorar la seguridad de los mismos mediante la aplicación de firmas del IPS
- Ser capaz de enviar archivos para **SOLUCIÓN** de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo
- Soportar método de equilibrio de carga y miembros del grupo
- Ser capaz de soportar políticas de enrutamiento de aplicaciones de capa 4/7
- Soportar Persistencia del servidor de capa 4/7
- Soportar balanceo de cargas de aplicaciones de carga 4-7 para:
  - TCP, UDP, IP, DNS, HTTP, HTTPS, HTTP 2.0 GW, FTP, SIP, RDP, RADIUS, MySQL, MSSQL, RTMP, RTSP.
  - Soportar cambios y reescritura de contenido L7 para:
    - Host HTTP, URL de solicitud HTTP y URL de referencia HTTP
    - Dirección IP origen
  - Soportar al menos:
    - IP persistente,
    - encabezado hash,
    - cookie persistente,
    - cookie hash,
    - hash de IP de destino,
    - hash de URI,
    - hash de URI completo,
    - hash de host
    - hash de dominio de host
- Soportar los siguientes métodos de Deployment:
  - Modo Router
  - Transparente
  - Alta disponibilidad
- Soportar NAT estática y dinámica
- Contar con las siguientes especificaciones técnicas:
  - Throughput de capa 4 de 15 Gbps
  - Throughput de capa 7 de 12 Gbps
  - Al menos 12 millones de Conexiones concurrentes en capa 4
  - Throughput de comprensión de 10 Gbps
  - Memoria interna de 32 Gb
  - Al menos 4 interfaces de cobre Rj45
  - Almacenamiento interno de 120 Gb
  - 2x 10 GE SFP+, 4x GE SFP, 4x GE RJ45 (Opcional)

## 8 SERVICIOS de DNS

### Descripción de los SERVICIOS:

El proveedor deberá brindar una **SOLUCIÓN** de seguridad para los Sistemas de Nombres de Dominio (DNS), mediante equipos de propósito específico, que solicita La **UNIVERSIDAD** debiendo cumplir las





siguientes especificaciones mínimas que permitan la comunicación, resolución y protección contra los ciberataques. Los equipos deberán brindar las siguientes funcionalidades mínimas:

### **Detalles de los SERVICIOS:**

#### **LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ**

- Ser de Hardware de propósito específico.
- Soportar administración remota.
- Soportar IPv4.
- Proporcionar monitoreo de fallas del sistema en tiempo real.
- Proporcionar monitoreo SNMP.
- Contar con capacidad de gestión de direcciones IP (IPAM)
- Contar con un mecanismo de administración vía interfaz Web.
- Incluir la funcionalidad de reinicios programados para los **SERVICIOS** DNS y DHC.
- Integrarse a una malla con tecnología de **SERVICIOS** patentada por el fabricante.
- Estar robustecida de fábrica (hardened).
- Utilizar un sistema operativo propietario.
- Tener la capacidad de integrarse con otro equipo de iguales características y modelo para ser instalados en alta disponibilidad en un arreglo activo y pasivo mediante un protocolo estándar como VRRP.

La **SOLUCIÓN no deberá** ofrecer el acceso a la línea de comandos root.

### **Características de los SERVICIOS de DNS:**

#### **LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ:**

- Tener la capacidad de proporcionar alta disponibilidad geográfica mediante el uso de Anycast para DNS.
- Permitir la creación de vistas de DNS y vistas de red.
- Permitir la configuración de DNSSEC
- Utilizar plantillas de nombres de host, que permitan aplicar normas de dichos nombres.
- Manejar:
  - RFC's para DNS: 1032, 1034, 1035, 1101, 1122, 1123, 1535, 1536, 1537, 1591, 1611, 1612, 1912, 1982,1995, 1996, 2052, 2136, 2168, 2181, 2308, 2317, 2537, 2671, 2782, 2845, 2915, 3596, 3645, 4033, 4034, 4035, 4641, 4956, 5155, 5702.
- Manejar y soportar los siguientes registros:
  - A (IPv4 Address)
  - NS (Name server)
  - AAAA (IPv6 Address)
  - PTR (Pointer)



- MX(Mailexchanger)
- TLSA (Transport Layer Security)
- CNAME (Canonical name)
- DNAME
- HOST
- Permitir la limpieza de DNS dinámicos basado en los siguientes criterios:
  - La fecha de creación del registro DNS
  - La fecha en la que se consultó por última vez el registro DNS
  - Atributos extensibles personalizables únicos para entornos de TI
  - Tipo de registros DNS
  - La **SOLUCIÓN** deberá soportar DNS64
- Mostrar tableros o paneles con información del estado que permitan mostrar:
  - Estadísticas de DNS como:
    - Success
    - NXDOMAIN
    - Referral
    - NXRRSET
    - Failure
    - Recursion
    - Monitoreo del sistema
    - Verificación de la integridad DNS

### Las características de protección con que deberá cumplir el SERVICIOS DNS:

#### LA SOLUCIÓN PROPUESTA POR EL LICITANTE DEBERÁ:

- La solución de DNS deberán ser capaces de minimizar las irrupciones del servicio de DNS causadas por ataques de DDoS y y otros ataques específicos de DNS.
- La solución debe detectar y mitigar de manera inteligente los ataques de DNS mientras responde solo a consultas legítimas mediante el uso de inteligencia de amenazas constantemente actualizada, sin necesidad de implementar parches de seguridad.

#### DNS Externo autoritativo con protección Avanzada de DNS

Equipos DNS Autoritativos Externos con Protección Avanzada de DNS. La **SOLUCIÓN** podrá cumplir con las características mencionadas como generales, y si además de:

- **SOLUCIÓN** para los equipos de DNS autoritativo externo puede integrarse a la malla de **SERVICIOS**.
- Está basada en equipos de propósito específico.
- La administración de la **SOLUCIÓN** de DNS Autoritativos Externos es realizada desde la consola de administración; que será el responsable de la coordinación y la sincronización de datos y configuraciones de los otros equipos que se designen como servidores de DNS.
- Su administración es granular y basada en Roles.
- Tienen soporte de IPv4 e IPv6 simultáneamente.
- Soporte ser monitoreados mediante SNMP.



- Permita la interconexión en la de los equipos de administración, de **SERVICIOS**, siendo todos los equipos del mismo fabricante.
- Utilice un sistema operativo propietario y robustecido de fábrica.
- Deberá soportar Anycast
- Configuración de DNSSEC (firmado y mantenimiento de las firmas de zonas) según NIST-800-81
- Capaces de manejar DNSSEC cubriendo los RFCs: 4033, 4034, 4035, 4641, 4956, 5155, 5702.
- Redirección y filtrado de DNS.
- RFCs: 1034, 1035, 2136, 1995, 1996, 2845, 2317.
- Capacidad de manejar vistas de DNS.
- La **SOLUCIÓN** para los equipos autoritativos externos deberá brindar monitoreo continuo, detección y mitigación de los siguientes tipos de ataques:
  - Reflexión de DNS / DrDoS.
  - Amplificación DNS.
  - Inundaciones de TCP / UDP / ICMP.
  - NXDOMAIN.
  - Random subdomain (ataques slow-drip).
  - Dominios Fantasma.
  - Exploits basados en DNS.
  - Envenenamiento de Cache de DNS.
  - Anomalías de protocolo.
  - Reconocimiento.
  - Secuestro de DNS.
  - Túneles de DNS.
- Las soluciones para los equipos autoritativos externos deberán utilizar tecnología para actualizar automáticamente la protección contra amenazas nuevas y cambiantes, utilizando la última inteligencia de amenazas, sin tiempo de inactividad o parches.
- Estos equipos para DNS Autoritativo externo se deberán instalar después de los firewalls y tienen la capacidad de auto-protegerse contra ataques específicos de DNS

## **9 SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)**

La **UNIVERSIDAD** requiere que el proveedor de los **SERVICIOS** cuente con un Centro de Operaciones de la Seguridad (SOC), que cuente con los certificados ISO9001, ISO22301, ISO27001 e ISO20000, que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro deberá de ser la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de **SERVICIOS**, administración de bitácoras, atención y respuesta a incidentes, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable sobre las soluciones propuestas.

Los **SERVICIOS** del SOC se refiere a las soluciones propuestas e implementadas por el proveedor, así mismo se deberá considerar que las bitácoras se basen en un **SERVICIO** de correlación de eventos e incidentes de seguridad donde los casos de uso deberán ser ilimitados, así como las respuestas ante un incidente alineadas a tiempo de los SLAs basado en los **SERVICIOS** solicitados en esta convocatoria.



### Detalles de los **SERVICIOS**:

- Ubicarse dentro de territorio mexicano (a fin de que se encuentre dentro de jurisdicción de las leyes mexicanas)
- Operación continua las 24 horas del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.
- Contar con personal para atención de los **SERVICIOS** en sitio y de forma remota, el cual se encuentre calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la **SOLUCIÓN**.
- Contar con un implant con las capacidades necesarias en las soluciones propuestas para ser el primer punto de contacto para la UNIVERSIDAD, en un horario de 8x5, con disponibilidad de horario en caso de incidentes.
- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.
- Infraestructura dedicada para la administración, operación y monitoreo de los componentes hardware y software que componen los **SERVICIOS** de seguridad.
- Realizar evaluaciones operativas a los **SERVICIOS** (herramienta de software y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software.
- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones de seguridad.
- Notificaciones y alertas, en caso de desviaciones, anomalías o brechas de seguridad.
- Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y Atención a fallas a los componentes hardware y software que integran la **SOLUCIÓN**, conforme lo estipulado en los acuerdos de niveles de **SERVICIOS**.
- Realizar mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada **SERVICIOS**.
- Ejecutar procesos operativos para al menos los siguientes rubros:
  - Administración de Monitoreo.
  - Administración de Cambios.
  - Administración de Configuraciones.
  - Administración de Vulnerabilidades.
  - Administración de Incidentes.
  - Administración de Problemas.
- Integrar una Mesa de **SERVICIOS** apegada a ITIL v4, la cual deberá integrarse con la Mesa de **SERVICIOS** Tecnológicos de la **UNIVERSIDAD**, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine la **UNIVERSIDAD**.
- El **SERVICIOS** de requerimientos, cambios, incidentes, entre otros, deberá permitir la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, podrán ser:
  - Un número telefónico directo en las instalaciones del SOC.
  - Correo Electrónico



- Portal Web
- El personal del proveedor que atenderá las operaciones de los **SERVICIOS** de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información, para lo cual, deberá integrarse el Currículum Vitae de todo el personal que participe en el **SERVICIOS**, indicando al menos:
  - **Experiencia profesional:** bajo este rubro, se considerarán todos los cargos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia al menos de 3 años.
  - **Estudios:** bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo “vendor-neutral”.
  - Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.
- Generar los reportes de desempeño de los **SERVICIOS** de seguridad. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:
  - Estadísticas de ataques informáticos bloqueados.
  - Estadísticas de comportamientos tipo esperado de uso por tecnología
- Proporcionar a la **UNIVERSIDAD** acceso a las soluciones de los **SERVICIOS** de seguridad, las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Las consolas de administración provistas para los **SERVICIOS** de seguridad deberán permitir visualizar al menos:
  - Políticas: Control de Acceso
  - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
  - Objetos: Usuarios, Grupos, Direcciones IP
  - Bitácoras.
  - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.

## 10 ENTREGABLES

Durante la habilitación, transición y operación de los **SERVICIOS** de seguridad, la **UNIVERSIDAD** requiere recibir distintos tipos de documentos, reportes o esquemas que favorezcan el desempeño y la continuidad de los **SERVICIOS**, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
<b>SERVICIOS</b> de habilitación de seguridad.	Plan de Trabajo Detallado de los <b>SERVICIOS</b> del proyecto	Única Vez	15 días naturales posterior a la emisión del fallo



SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
	Matriz de Escalación	Única Vez	15 días naturales posterior a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los <b>SERVICIOS</b>	Única Vez	15 días naturales posterior a la emisión del fallo
<b>SERVICIOS</b> de Seguridad.	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada <b>SERVICIOS</b> que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada <b>SERVICIOS</b> que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes
	Memorias Técnicas Actualizadas de las <b>SERVICIOS</b> de Seguridad	Única Vez	20 días hábiles previo al término del contrato para aquellos <b>SERVICIOS</b> que se encuentren habilitados
<b>SERVICIOS</b> del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: <ul style="list-style-type: none"><li>• Requerimientos</li><li>• Cambios</li><li>• Configuraciones</li><li>• Incidentes</li><li>• Problemas</li><li>• Monitoreo</li></ul>	Única Vez	15 días naturales posterior a la emisión del fallo



SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la emisión del fallo
	Procedimiento de operación de la Mesa de <b>SERVICIOS</b> : <ul style="list-style-type: none"> <li>• Requerimientos</li> <li>• Cambios</li> <li>• Configuraciones</li> <li>• Incidentes</li> <li>• Problemas</li> <li>• Monitoreo</li> </ul>	Única Vez	15 días naturales posterior a la emisión del fallo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior a la emisión del fallo

### 11 Entregables bajo demanda

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los **SERVICIOS** de seguridad, que incluya al menos los siguientes conceptos:

SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
<b>SERVICIOS</b> del Centro de Operaciones de Seguridad y Red (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posterior al término de la implementación de cualquier <b>SOLUCIÓN</b> de seguridad
	Actualización de la matriz de escalación	Evento	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad.	Evento	5 días hábiles posterior a la ejecución de la ventana mantenimiento
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte de la <b>UNIVERSIDAD</b>





SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte de la <b>UNIVERSIDAD</b>
	Reporte Técnico de los requerimientos registrados en la mesa de <b>SERVICIOS</b>	Evento	5 días hábiles posterior a la solicitud generada por parte de la <b>UNIVERSIDAD</b>
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del <b>UNIVERSIDAD</b>

## 12 Entregables Periódicos

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los **SERVICIOS** de seguridad, que incluya al menos los siguientes conceptos:

SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
<b>SERVICIOS</b> de Seguridad	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none"> <li>• Disponibilidad</li> <li>• Controles de Cambios</li> <li>• Requerimientos</li> <li>• Incidentes/Fallas</li> <li>• Actividad Sospechosa</li> <li>• Estadísticas de uso de los <b>SERVICIOS</b></li> </ul>	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
<b>SERVICIOS</b> del Centro de Operaciones de Seguridad y Red (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de <b>SERVICIOS</b> para los <b>SERVICIOS</b> de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los	Mensual	5 días hábiles posterior al





SERVICIOS	ENTREGABLE	PERIODICIDAD	ENTREGA
	<b>SERVICIOS</b> de seguridad y red implementados		cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los <b>SERVICIOS</b> de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los <b>SERVICIOS</b> de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido

Los entregables proporcionados durante las etapas de implementación, transición y operación de los **SERVICIOS** de seguridad, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por la **UNIVERSIDAD**.

De igual manera, el proveedor deberá establecer un repositorio digital, que de manera alterna, servirá para depositar los entregables antes señalados, mismo que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que la **UNIVERSIDAD** definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionarios que sean designados por el primero mencionado.

### **SERVICIOS de Habilitación de las soluciones de seguridad.**

DESCRIPCIÓN DEL NIVEL DE SERVICIOS	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Plan de Trabajo detallado de los <b>SERVICIOS</b> del proyecto	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Matriz de Escalación	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades,	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento



competencias y capacidades para soportar la prestación de los <b>SERVICIOS</b>			
--	--	--	--

### SERVICIOS de Seguridad informática

DESCRIPCIÓN DEL NIVEL DE SERVICIOS	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique la <b>UNIVERSIDAD</b>	5 días hábiles posteriores a la integración de las mesas de trabajo por cada <b>SERVICIOS</b> que se pretenda habilitar	0.9% por cada día hábil de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique la <b>UNIVERSIDAD</b>	10 días hábiles posteriores a la integración de las mesas de trabajo por cada <b>SERVICIOS</b> que se pretenda habilitar	0.9% por cada día hábil de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique la <b>UNIVERSIDAD</b> , conforme cada <b>SOLUCIÓN</b> integrada y posterior a la integración de las mesas de trabajo	0.9% por cada día hábil de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Memorias Técnicas Actualizadas de las <b>SERVICIOS</b> de Seguridad	20 días hábiles previo al término del contrato para aquellos <b>SERVICIOS</b> que se encuentren habilitados	0.9% por cada día hábil de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

### SERVICIOS del Centro de Operaciones de Seguridad (SOC)



DESCRIPCIÓN DEL NIVEL DE SERVICIOS	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	CÓMPUTO DE LA PENALIZACIÓN
Procesos de operación implementados: <ul style="list-style-type: none"><li>• Requerimientos</li><li>• Cambios</li><li>• Configuraciones</li><li>• Incidentes</li><li>• Problemas</li><li>• Monitoreo</li></ul>	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Expedientes Curriculares del personal del SOC	15 días naturales posterior a la emisión del fallo	0.9% por cada día natural de atraso	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

### 13 Deducciones

Durante la vida del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al **SERVICIOS** asociado no será aplicada al proveedor, siempre y cuando demuestre con evidencias fehacientes que el **SERVICIOS** afectado no deriva del proveedor ganador.

### 14 Disponibilidad

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el **SERVICIOS** de seguridad informática (o un componente del sistema) realiza la función que le es propia. Es decir; disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

Las mediciones de disponibilidad deberán ser realizadas por el Proveedor usando su correspondiente herramienta de monitoreo de los **SERVICIOS**, con el afán de obtener mediciones precisas con respecto a los tiempos operacionales.

Las caídas originadas por falla de energía responsabilidad de la **UNIVERSIDAD** no serán tomadas en cuenta para la disponibilidad.



Disponibilidad de los **SERVICIOS** =  $[\text{Tiempo Total} - (\text{Tiempo indisponible} - \text{Tiempo UNIVERSIDAD}) / \text{Tiempo total}] \times 100$

Dónde:

Tiempo Total: Tiempo total de disponibilidad para el mes de medición.

Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.

Tiempo **UNIVERSIDAD**: Tiempos atribuibles al **UNIVERSIDAD** extraídos del sistema de administración de incidentes.

### 15 Objetivos por métrica:

Disponibilidad <b>SERVICIOS</b>	% Disponibilidad
<b>SERVICIOS</b> de Seguridad informática	99.95%
<b>SERVICIOS</b> del Centro de Operaciones de Seguridad (SOC)	99.99%

### 16 Deductiva por incumplimiento:

DESCRIPCIÓN DEL NIVEL DE SERVICIOS	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Cuando no se cumplan con los objetivos de <b>SERVICIOS</b> , para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto	% Disponibilidad conforme la tabla de objetivos	0.9% por cada día de indisponibilidad	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

### 17 Tiempo de Detección y SOLUCIÓN de Fallas

La métrica de tiempo de **SOLUCIÓN** a fallas es independiente de la métrica de disponibilidad, dado que se refiere al tiempo en el cual será devuelta a la normalidad (restitución de la operación estable) uno o varios **SERVICIOS** al presentarse una falla. Las mediciones de Tiempo de **SOLUCIÓN** de Fallas deberán ser realizadas por el Proveedor.

El Tiempo de **SOLUCIÓN** a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

**Severidad Crítica:** Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y **SERVICIOS** del cliente. Eventos de afectación total al **SERVICIOS**, pérdida total del sistema seguridad, degradación de los recursos de la **UNIVERSIDAD** o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida.



**Severidad Alta:** Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los **SERVICIOS** e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos **SERVICIOS** de seguridad informática.

**Severidad Media:** Representa un incidente menor que no trae consecuencias de impacto de negocio a los **SERVICIOS** e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas de **SERVICIOS** internos de la **UNIVERSIDAD** y hacia un grupo reducido de usuarios.

**Severidad Baja:** Son casos considerados como preventivos para fines de mejora u optimización de cualquier **SERVICIOS** de seguridad. Estos casos de severidad deberán ser atendidos por ingenieros del proveedor de **SERVICIOS** con la colaboración del fabricante vía un centro de asistencia técnica personalizada.

La severidad de un incidente es determinada por la convocante. Conforme la operación y criticidad de un **SERVICIOS**, se define la severidad, así como su nivel de escalación, con base en lo siguiente:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa una falla de alto impacto que impide la operación total de un <b>SERVICIOS</b> , mismo que soporta una función de la <b>UNIVERSIDAD</b> .	10 minutos posterior a la detección de la falla	2 horas posterior al registro y notificación de la falla
Alta	Representa una falla en la que hay una degradación que impide la operación de un <b>SERVICIOS</b> , mismo que soporta una función de la <b>UNIVERSIDAD</b> .	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Representa una falla menor que impide la operación de un <b>SERVICIOS</b> , mismo que afecta a un grupo de usuarios reducido de la <b>UNIVERSIDAD</b> .	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier <b>SERVICIOS</b> de seguridad informática, tienen un bajo impacto en la operación y su atención y/o <b>SOLUCIÓN</b> puede ser calendarizada.	5 días hábiles posterior a la detección de la falla	Se define entre la <b>UNIVERSIDAD</b> y el Proveedor.

## 18 Deductiva por incumplimiento:

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIOS)	NIVEL DE SERVICIOS	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y	10 minutos posterior al	Días	0.9% por cada día de atraso en el	Valor unitario de la facturación mensual



notificación conforme al nivel de severidad critica	registro y notificación de la falla		registro y notificación	de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad critica	2 horas posterior al registro y notificación de la falla	Días	0.9% por cada día o fracción de atraso en la <b>SOLUCIÓN</b> de la falla	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación de la falla	Días	0.9% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad alta	4 horas posterior a la registro y notificación de la falla	Días	0.9% por cada día o fracción de atraso en la <b>SOLUCIÓN</b> de la falla	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	120 minutos posterior al registro y notificación de la falla	Días	0.6% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad media	48 horas posterior al registro y notificación de la falla	Días	0.6% por cada día o fracción de atraso en la <b>SOLUCIÓN</b> de la falla	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	5 días hábiles posterior al registro y notificación de la falla	Días	0.1% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad baja	Se define entre la <b>UNIVERSIDAD</b> y el Proveedor.	Días	0.1% por cada día o fracción de atraso en la <b>SOLUCIÓN</b> de la falla	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

## 19 Tiempo de Detección y Mitigación de Incidentes

Una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad informática y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad.



Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envío de dictamen que el proveedor deberá realizar ante la **UNIVERSIDAD** al momento de detectar una actividad sospechosa.

Ante una actividad sospechosa, el proveedor deberá registrar y notificar al personal de la **UNIVERSIDAD** en máximo 48 hrs. Posterior a su detección y registro, se deberá emitir un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal de la **UNIVERSIDAD** en máximo 72 hrs.

## 20 Objetivos de la métrica:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa un incidente de alto impacto que impide la operación total de un <b>SERVICIOS</b> , mismo que soporta una función de la <b>UNIVERSIDAD</b>	10 minutos posterior a la detección del incidente	1 hora posterior al registro y notificación del incidente
Alta	Representa un incidente en el que hay una degradación que impide la operación de un <b>SERVICIOS</b> , mismo que soporta una función de la <b>UNIVERSIDAD</b> .	20 minutos posterior a la detección del incidente	4 horas posterior al registro y notificación del incidente
Media	Representa un incidente menor que impide la operación de un <b>SERVICIOS</b> , mismo que afecta a un grupo de usuarios reducido de la <b>UNIVERSIDAD</b> .	30 minutos posterior a la detección del incidente	24 horas posterior al registro y notificación del incidente
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier <b>SERVICIOS</b> de seguridad, tienen un bajo impacto en la operación de la <b>UNIVERSIDAD</b> y su	60 minutos posterior a la detección del incidente	48 horas posterior al registro y notificación del incidente





	atención y/o <b>SOLUCIÓN</b> puede ser calendarizada.		
--	---	--	--

**21 Deductiva por incumplimiento:**

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIOS)	NIVEL DE SERVICIOS	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Registro y notificación de Actividad Sospechosa	60 minutos posterior a la detección actividad sospechosa	Día	0.9% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Envío de Dictamen de Actividad Sospechosa	72 horas posterior al registro y notificación de actividad sospechosa	Día	0.9% por cada día de atraso en la elaboración del dictamen	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIOS)	NIVEL DE SERVICIOS	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posterior al registro y notificación del incidente	Día	0.9% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad critica	60 minutos posterior al registro y notificación del incidente	Día	0.9% por cada día de atraso en la <b>SOLUCIÓN</b> del incidente	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación del incidente	Día	0.9% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad alta	240 minutos posterior al registro y	Día	0.9% por cada día de atraso en la <b>SOLUCIÓN</b> del incidente	Valor unitario de la facturación mensual de los <b>SERVICIOS</b>





	notificación del incidente			relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	30 minutos posterior al registro y notificación del incidente	Día	0.6% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad media	1,440 minutos posterior al registro y notificación del incidente	Día	0.6% por cada día de atraso en la <b>SOLUCIÓN</b> del incidente	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	60 minutos posterior al registro y notificación del incidente	Día	0.1% por cada día de atraso en el registro y notificación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Tiempo máximo de <b>SOLUCIÓN</b> conforme al nivel de severidad baja	2,880 minutos posterior al registro y notificación del incidente	Día	0.1% por cada día de atraso en la <b>SOLUCIÓN</b> del incidente	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

## 22 **SERVICIOS** del Centro de Operaciones de Seguridad (SOC)

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIOS)	NIVEL DE SERVICIOS	UNIDAD DE MEDIDA	DEDUCTIVA	LIMITE DE INCUMPLIMIENTO
Reporte Técnico de los requerimientos generados a través del SOC para los <b>SERVICIOS</b> de seguridad informática implementados	5 días hábiles posterior al cumplimiento del mes vencido	Día	0.9% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reporte Técnico de los controles de cambios generados para los <b>SERVICIOS</b> de seguridad informática implementados	5 días hábiles posterior al cumplimiento del mes vencido	Día	0.9% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento



Reporte Técnico de los incidentes presentados en los <b>SERVICIOS</b> de seguridad informática implementados	5 días hábiles posterior al cumplimiento del mes vencido	Día	0.9% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reporte Técnico de los eventos de actividad sospechosa presentados en los <b>SERVICIOS</b> de seguridad informática implementados	5 días hábiles posterior al cumplimiento del mes vencido	Día	0.9% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reporte de las evaluaciones operativas a los <b>SERVICIOS</b> de seguridad informática implementados	5 días hábiles posterior al cumplimiento de cada trimestre vencido	Día	0.9% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Actualización de la matriz de escalación	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad	Día	0.9% por cada día hábil de atraso en la entrega de la matriz de escalación	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad informática.	5 días hábiles posterior a la ejecución de la ventana mantenimiento	Día	0.9% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en las soluciones de seguridad informática	5 días hábiles posterior a la solicitud generada por parte de la <b>UNIVERSIDAD</b>	Día	0.9% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Reporte Técnico de los requerimientos	5 días hábiles posterior a la	Día	0.9% por cada día hábil de atraso en	Valor unitario de la facturación



registrados en el SOC	solicitud generada por parte de la <b>UNIVERSIDAD</b>		la entrega del reporte técnico	mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento
Diagramas de Arquitectura de las soluciones de seguridad informática	5 días hábiles posterior a la solicitud generada por parte de la <b>UNIVERSIDAD</b>	Día	0.9% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual de los <b>SERVICIOS</b> relacionado con el incumplimiento

Cualquier cambio ejecutado por el **SOC**, mismo que no se encuentre autorizado por la **UNIVERSIDAD**, derive o no en alguna falla de los **SERVICIOS** de seguridad informática, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

### 23 Perfiles

A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto:

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Administrador del Centro de Operaciones de Seguridad (SOC)	CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional)	5 años de experiencia en participación de proyectos de seguridad de la información.	Responsable de la administración, monitoreo, operación de los <b>SERVICIOS</b> proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad.	Al menos 1 recurso
Analista de Seguridad	CEH (Certified Ethical Hacker)	5 años de experiencia en participación de proyectos de seguridad de la información.	Encargado de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	Al menos 2



PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	5 años de experiencia en participación de proyectos de seguridad de la información.	Es la persona encargada de administrar y coordinar el proyecto.	Al menos 1
Operador de la mesa de <b>SERVICIOS SOC</b>	ITIL v4 Foundation Certification	3 años de experiencia en participación de proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los <b>SERVICIOS</b> , así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos.	Al menos 4
Arquitecto Especializado en Redes y Seguridad	CCNP (Cisco Certified Network Professional) o CCSP (Cisco Certified Security Professional)	3 años de experiencia en participación de proyectos de redes y seguridad de la información.	Responsable de la administración, monitoreo, operación de los <b>SERVICIOS</b> proporcionados por el SOC, en lo que a <b>SERVICIOS</b> de interconexión de red se refiere, así como del soporte, atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes.	Al menos 1 recurso



PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Analista y operador de Seguridad en sitio.	Qué acredite con certificaciones o constancias conocer soluciones en ciberseguridad y/o soluciones de red	Minimo 3 años de experiencia.	<p>Encargado de ejecutar en 1er nivel la revisión de infraestructura de seguridad propuesta, dar seguimiento a la falla hasta solución.</p> <p>Ser el 1er punto de contacto ante el SOC para diagnostico y validaciones en sitio sobre las soluciones propuestas en la convocatoria.</p> <p>Encargado de ejecutar las actividades que requiere ventanas de mantenimiento (preventivo/correctivo) en las soluciones de seguridad propuestas.</p> <p>Participar en ventanas programadas con el cliente en actividades que impliquen cambios y que estos afecten las soluciones de seguridad propuestas.</p> <p>Encargado de levantar los ticktes de seguimiento con el SOC ante un incidente de seguridad y que intervengan las soluciones de seguridad propuestas.</p>	Un recurso



**ANEXO NÚM. 1**

(UTILIZAR PAPEL MEMBRETADO DEL LICITANTE)

**PROPUESTA TÉCNICA**

LUGAR Y FECHA

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

CON RELACIÓN A LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, ME PERMITO PONER A SU CONSIDERACIÓN LA SIGUIENTE PROPUESTA TÉCNICA:

PARTIDA	DESCRIPCIÓN DE LOS BIENES Y/O SERVICIOS	UNIDAD	CANTIDAD
UNICA	LA DESCRIPCIÓN PORMENORIZADA DE LOS <b>SERVICIOS</b> Y SUS ESPECIFICACIONES DETALLADAS QUE OFERTA EL <b>LICITANTE</b> , DEBERÁ SER TOTALMENTE COINCIENTES CON EL <b>ANEXO A. ANEXO TÉCNICO. ESPECIFICACIONES TÉCNICAS DETALLADAS PARA LOS "SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMATICA"</b> DE LA CONVOCATORIA. Y LAS MODIFICACIONES QUE PUDIERAN DERIVARSE DE LA JUNTA DE ACLARACIÓN DE DUDAS.	<b>SERVICIOS</b>	1

\_\_\_\_\_  
FIRMA DEL **LICITANTE** O APODERADO LEGAL



**ANEXO No. 2**

(UTILIZAR PAPEL MEMBRETADO DEL LICITANTE)

**PROPUESTA ECONÓMICA**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

CON RELACIÓN A LA LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA, ME PERMITO PONER A SU CONSIDERACIÓN LA SIGUIENTE PROPUESTA ECONÓMICA: SEGÚN ESPECIFICACIONES CONTENIDAS EN EL ANEXO 1 DE MI PROPUESTA

**HOJA DE COTIZACIÓN**

DESCRIPCIÓN SIMPLIFICADA DEL CONCEPTO	CANTIDAD	IMPORTE MENSUAL TOTAL (M.N.) ANTES DE I.V.A.	IMPORTE TOTAL (M.N.) ANTES DE I.V.A.
Habilitación del SERVICIOS de seguridad.			
SERVICIOS de seguridad.			
SERVICIOS del Centro de Operaciones de Seguridad (SOC)			
<b>TOTAL DE LA PROPUESTA</b>	<b>SUBTOTAL</b>		
	<b>I.V.A</b>		
	<b>TOTAL</b>		

**IMPORTE TOTAL CON LETRA:**

LOS PRECIOS DE LA PRESENTE COTIZACIÓN SERÁN FIRMES, DURANTE TODA LA VIGENCIA DEL CONTRATO, Y TENDRÁN UNA VALIDEZ DE 30 (TREINTA) DÍAS NATURALES, A PARTIR DE LA FECHA DE APERTURA DE PROPUESTAS.

**A T E N T A M E N T E**

**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



**ANEXO No. 3**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**CARTA DE MANIFESTACIÓN DE INTERÉS DE PARTICIPACIÓN Y ACREDITACIÓN DE PERSONALIDAD**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

(NOMBRE) \_\_\_\_\_, MANIFIESTO BAJO PROTESTA DE DECIR VERDAD, QUE LOS DATOS AQUÍ ASENTADOS, SON CIERTOS Y HAN SIDO DEBIDAMENTE VERIFICADOS, ASÍ COMO QUE CUENTO CON FACULTADES SUFICIENTES PARA MANIFESTAR INTERÉS EN PARTICIPAR EN LA PRESENTE **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, A NOMBRE Y REPRESENTACIÓN DE: (**LICITANTE**)\_\_\_\_\_.

NÚMERO DEL REGISTRO FEDERAL DE CONTRIBUYENTES: \_\_\_\_\_

NOMBRE DEL APODERADO O REPRESENTANTE LEGAL: \_\_\_\_\_

DOMICILIO:

CALLE \_\_\_\_\_ NÚMERO \_\_\_\_\_ COLONIA \_\_\_\_\_ C.P. \_\_\_\_\_ DELE

GACIÓN O MUNICIPIO \_\_\_\_\_ ENTIDAD FEDERATIVA \_\_\_\_\_

TELÉFONO \_\_\_\_\_ CORREO ELECTRÓNICO \_\_\_\_\_

**TRATÁNDOSE DE PERSONAS MORALES:**

NÚMERO DE LA ESCRITURA PÚBLICA \_\_\_\_\_; FECHA EN LA QUE CONSTA EL ACTA CONSTITUTIVA \_\_\_\_\_; NOMBRE DEL NOTARIO PÚBLICO \_\_\_\_\_

NÚMERO \_\_\_\_\_ Y LUGAR ANTE EL CUAL SE DIO FE DE LA MISMA, CON EL REGISTRO PÚBLICO NO. \_\_\_\_\_

**RELACIÓN DE LOS ACCIONISTAS:**

APELLIDO PATERNO \_\_\_\_\_





APELLIDO MATERNO _____	_____	_____
NOMBRE (S) _____	_____	_____
DESCRIPCIÓN DEL OBJETO SOCIAL DE LA EMPRESA:		
_____		
REFORMAS AL ACTA CONSTITUTIVA Y SU NÚMERO DE REGISTRO PÚBLICO:		
_____		

**DEL REPRESENTANTE DEL LICITANTE**

<b>NOMBRE DEL REPRESENTANTE O APODERADO LEGAL:</b>
NÚMERO _____ Y FECHA _____ DE LA ESCRITURA PÚBLICA EN LA QUE CONSTA QUE CUENTA CON FACULTADES SUFICIENTES PARA SUSCRIBIR LA PROPUESTA; EL NOMBRE DEL NOTARIO PÚBLICO _____ Y NÚMERO _____, ANTE EL CUAL FUE OTORGADA.

**PROTESTO LO NECESARIO**

\_\_\_\_\_

(FIRMA)



**ANEXO No. 4**  
**(UTILIZAR PAPEL MEMBRETADO DEL LICITANTE)**  
**FORMATO DE CARTA PODER SIMPLE**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

\_\_\_\_\_ ( NOMBRE DEL LICITANTE ) BAJO PROTESTA DE DECIR VERDAD EN MI CARÁCTER DE ( CARÁCTER QUE OSTENTA QUIEN OTORGA EL PODER ) DE LA EMPRESA ( NOMBRE DE LA EMPRESA LICITANTE ) SEGÚN CONSTA EN EL TESTIMONIO NOTARIAL NÚMERO \_\_\_\_\_ OTORGADO ANTE NOTARIO PÚBLICO N° \_\_\_\_\_ DE LA ( CIUDAD EN QUE SE OTORGO EL INSTRUMENTO NOTARIAL ) Y DE APLICAR EL NÚMERO DE REGISTRO( \_\_\_\_\_ ), POR ESTE CONDUCTO Y FACULTADO PARA ELLO, AUTORIZO A ( NOMBRE DE QUIEN ACEPTA EL PODER ) PARA: QUE A NOMBRE DE MI REPRESENTADA, SE ENCARGUE DE LAS SIGUIENTES GESTIONES: PARTICIPAR EN LA JUNTA DE ACLARACIÓN DE DUDAS A LAS BASES, ENTREGAR Y RECIBIR DOCUMENTACIÓN, PARTICIPAR EN EL ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES TÉCNICAS Y ECONÓMICAS, ASÍ COMO DE FALLO, Y HACER LAS ACLARACIONES QUE SE DERIVEN DE DICHS ACTOS, CORRESPONDIENTES DE LA LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 **SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**

\_\_\_\_\_  
(LUGAR Y FECHA)

OTORGA EL PODER

ACEPTA EL PODER

\_\_\_\_\_  
(NOMBRE, DOMICILIO Y FIRMA)

\_\_\_\_\_  
(NOMBRE, DOMICILIO Y FIRMA)

T E S T I G O S

\_\_\_\_\_  
(NOMBRE, DOMICILIO Y FIRMA)

\_\_\_\_\_  
(NOMBRE, DOMICILIO Y FIRMA)

**CARTA PODER SIMPLE FIRMADA ANTE DOS TESTIGOS, SÓLO EN EL CASO DE QUE NO ASISTA EL LICITANTE, SU REPRESENTANTE LEGAL O PERSONA FACULTADA, CON ORIGINAL Y COPIA SIMPLE DE LA IDENTIFICACIÓN OFICIAL VIGENTE (CREDENCIAL PARA VOTAR CON FOTOGRAFÍA O CARTILLA DEL SERVICIOS MILITAR NACIONAL O CÉDULA PROFESIONAL O PASAPORTE) TANTO DEL PODERDANTE COMODEL ACEPTANTE DEL PODER, Y ÚNICAMENTE COPIA SIMPLE DE LA IDENTIFICACIÓN OFICIAL DE LOS TESTIGOS.**



**ANEXO No. 5**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**CARTA DE CONOCIMIENTO DEL CONTENIDO DE LA CONVOCATORIA**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

ME REFIERO A LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, SOBRE EL PARTICULAR MANIFIESTO A USTED QUE:

OPORTUNAMENTE SE TUVO CONOCIMIENTO DE LA CONVOCATORIA RELATIVA A LA LICITACIÓN PÚBLICA NACIONAL EN CUESTIÓN, Y **SE HA TENIDO DEBIDO CONOCIMIENTO DEL CONTENIDO DE LA MISMA, ACEPTÁNDOSE ÍNTEGRAMENTE LOS REQUISITOS ESTABLECIDOS EN LAS CITADAS BASES, LAS MODIFICACIONES QUE SE DERIVEN DE LA JUNTA DE ACLARACIÓN DE DUDAS A LAS BASES, ASÍ COMO EN EL O LOS CONTRATOS QUE SE SUSCRIBAN.**

DE IGUAL FORMA MANIFIESTO QUE SE CONOCE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA, Y DEMÁS DISPOSICIONES APLICABLES Y ACEPTA QUE ESTA NORMATIVIDAD RIGE EN LO CONDUCENTE.

**A T E N T A M E N T E**

---

**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



---

**ANEXO No. 6**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**CARTA MANIFIESTO DE NO ENCONTRARSE EN LOS SUPUESTOS QUE ESTABLECEN LOS ARTÍCULOS 60 Y 83 PENÚLTIMO PÁRRAFO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA.**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

CON RELACIÓN A LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA** MANIFIESTO BAJO PROTESTA DE DECIR VERDAD, NO ENCONTRARME EN NINGUNO DE LOS SUPUESTOS QUE ESTABLECEN LOS ARTÍCULOS 60 Y 83 PENÚLTIMO PÁRRAFO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA.

**A T E N T A M E N T E**

---

**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



---

**ANEXO No. 7**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**CARTA DE DECLARACIÓN DE INTEGRIDAD**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

POR ESTE CONDUCTO, YO, (NOMBRE DEL REPRESENTANTE LEGAL) EN MI CARÁCTER DE REPRESENTANTE LEGAL DE (NOMBRE DEL LICITANTE), MANIFIESTO EL ABSTENERME POR MI O POR INTERPÓSITAS PERSONAS, DE ADOPTAR CONDUCTAS PARA QUE LOS SERVIDORES PÚBLICOS DE **LA UNIVERSIDAD**, INDUZCAN O ALTEREN LAS EVALUACIONES DE LAS PROPUESTAS, EL RESULTADO DEL PROCEDIMIENTO U OTROS ASPECTOS QUE ME OTORGUEN CONDICIONES MÁS VENTAJOSAS CON RELACIÓN A LOS DEMÁS PARTICIPANTES EN LA **licitación pública nacional NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA.**

**ATENTAMENTE**

---

**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



---

**ANEXO No. 8**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**GARANTÍA DE LA INFRAESTRUCTURA**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

CON RELACIÓN A LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, EN MI CALIDAD DE **EL LICITANTE** O UREPRESENTANTE LEGAL DE LA EMPRESA \_\_\_\_\_, MANIFIESTO A USTED BAJO PROTESTA DE DECIR VERDAD QUE:

LOS EQUIPOS PROPUESTOS POR EL FABRICANTE, SON NUEVOS Y NO SE ENCUENTRAN CON ANUNCIO DE FIN DE VIDA.

DE IGUAL FORMA, ME COMPROMETO A OTORGAR A **LA UNIVERSIDAD** UNA GARANTÍA POR DEFECTOS DE FABRICACIÓN Y/O VICIOS OCULTOS, HASTA POR \_\_\_\_\_, CONTADOS A PARTIR DE LA FECHA DE ACEPTACIÓN DE LOS **SERVICIOS** POR PARTE DE LA DIRECCIÓN DE CONTROL DE BIENES E INVENTARIOS.

**ATENTAMENTE**

\_\_\_\_\_  
**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



---

**ANEXO No. 9**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**PROPIEDAD INDUSTRIAL Y DERECHOS DE AUTOR**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

CON RELACIÓN A LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA, EL LICITANTE (O SU REPRESENTANTE LEGAL)**  
\_\_\_\_\_, MANIFIESTO A USTED BAJO PROTESTA DE DECIR VERDAD QUE:

CONFORME AL NUMERAL (2.4 Y 5.2.c) DE LAS BASES, CON EL PRESENTE ME RESPONSABILIZO EXPRESAMENTE EN LOS CASOS EN QUE CON MOTIVO DEL SUMINISTROS DE LOS **SERVICIOS** OBJETOS DE ÉSTA LICITACIÓN, SE INFRINJAN PATENTES O MARCAS O VIOLE REGISTROS DE DERECHOS EXCLUSIVOS Y/O INHERENTES A LA PROPIEDAD, QUEDANDO LIBERADO DE ELLO A **LA UNIVERSIDAD**.

**A T E N T A M E N T E**

\_\_\_\_\_  
**NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL**



**ANEXO No. 10**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE  
ESTRATIFICACIÓN DE EMPRESAS (MIPYMES)**

LUGAR Y FECHA.

**M.C. SALVADOR PÉREZ MARTÍNEZ**

PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

ME REFIERO AL PROCEDIMIENTO DE LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA, EN EL QUE MI REPRESENTADA, LA EMPRESA \_\_\_\_\_ PARTICIPA A TRAVÉS DE LA PROPUESTA QUE SE CONTIENE EN EL PRESENTE SOBRE.

SOBRE EL PARTICULAR, Y EN LOS TÉRMINOS DE LO PREVISTO POR LOS “LINEAMIENTOS PARA FOMENTAR LA PARTICIPACIÓN DE LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS EN LOS PROCEDIMIENTOS DE ADQUISICIÓN Y ARRENDAMIENTO DE BIENES MUEBLES” ASÍ COMO LA “CONTRATACIÓN DE SERVICIOS QUE REALICEN LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL”, DECLARO BAJO PROTESTA DE DECIR VERDAD, QUE MI REPRESENTADA PERTENECE AL SECTOR (1), CUENTA CON (2) EMPLEADOS DE PLANTA REGISTRADOS ANTE EL IMSS Y CON (3) PERSONAS SUBCONTRATADAS Y QUE EL MONTO DE LAS VENTAS ANUALES DE MI REPRESENTADA ES DE (4) OBTENIDO EN EL EJERCICIO FISCAL CORRESPONDIENTE A LA ÚLTIMA DECLARACIÓN ANUAL DE IMPUESTOS FEDERALES. CONSIDERANDO LO ANTERIOR, MI REPRESENTADA SE ENCUENTRA EN EL RANGO DE UN EMPRESA (5), ATENDIENDO A LO SIGUIENTE:

Tamaño (5)	Sector (1)	Rango de número de trabajadores (2) + (3)	Rango de monto de ventas anuales (mdp) (4)	Tope máximo combinado *
Micro	Todas	Hasta 10	Hasta \$4	4.6
Pequeña	Comercio	Desde 11 hasta 30	Desde \$4.01 hasta \$100	93
	Industria y <b>SERVICIOS</b>	Desde 11 hasta 50	Desde \$4.01 hasta \$100	95
Mediana	Comercio	Desde 31 hasta 100	Desde \$100.01 hasta \$250	235
	<b>SERVICIOS</b>	Desde 51 hasta 100		
	Industria	Desde 51 hasta 250	Desde \$100.01 hasta 250	250

Tope máximo combinado = (trabajadores) x 10% + (ventas anuales x 90%)

(2) y (3) El número de trabajadores será el que resulte de la sumatoria de los puntos (2) y (3)

(5) El tamaño de la empresa se determinará a partir del puntaje obtenido conforme a la siguiente fórmula:

Puntaje de la empresa = (número de trabajadores) x 10% + (monto de ventas anuales) x 90% el cual debe ser igual o menor al tope máximo combinado de su categoría.

Asimismo, manifiesto, bajo protesta de decir verdad, que el Registro Federal de Contribuyentes de mi representada es:

**ATENTAMENTE**

\_\_\_\_\_  
NOMBRE Y FIRMA DE EL LICITANTE O SU REPRESENTANTE LEGAL





**ANEXO No. 11**

(Se trata de transcribir el texto íntegro de este formato de fianza en papel membretado del LICITANTE, en señal de que está de acuerdo que en caso de resultar adjudicado, este será el tipo y texto de la fianza a entregar)

**FORMATO DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.**

FECHA DE EXPEDICIÓN

**NOMBRE DE LA AFIANZADORA:**

*DECLARACIÓN EXPRESA DE QUE LA INSTITUCIÓN NACIONAL AFIANZADORA CUENTA CON LA AUTORIZACIÓN DE LA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO.*

**NUMERO DE PÓLIZA:**

*DECLARACIÓN DE QUE LA INSTITUCIÓN AFIANZADORA SE CONSTITUYE HASTA POR LA SUMA DE \$ (LETRA), EN MONEDA NACIONAL. A FAVOR DE LA **UNIVERSIDAD AUTÓNOMA DE SINALOA**.*

*PARA GARANTIZAR POR (NOMBRE Y DIRECCIÓN DE LA PERSONA FÍSICA O MORAL QUE SE OBLIGA), EL FIEL Y EXACTO CUMPLIMIENTO DE LAS OBLIGACIONES CONTENIDAS EN EL CONTRATO NO. \_\_\_\_\_ DE FECHA \_\_\_\_, DERIVADO DE LA **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, ASÍ MISMO, ESTA FIANZA SE OTORGA ATENDIENDO A TODAS LAS ESTIPULACIONES CONVENIDAS EN LAS BASES Y EN EL CONTRATO, LA MISMA ESTARÁ VIGENTE POR UN PERÍODO DE 12 MESES POSTERIORES A LA FECHA DE LA VIGENCIA DEL CONTRATO PARA GARANTIZAR LA CALIDAD DE LOS **SERVICIOS**, CONTRA DEFECTOS DE FABRICACIÓN Y/O VICIOS OCULTOS, POR UN PERÍODO DE 12 MESES, CONTADOS A PARTIR DE SU ACEPTACIÓN POR PARTE DE **LA UNIVERSIDAD** (DECLARACIÓN DE QUE LA FIANZA SE DEVOLVERÁ PARA SU CANCELACIÓN MEDIANTE MANIFESTACIÓN POR ESCRITO DE **LA UNIVERSIDAD** ASÍ COMO DE QUE EL CONTRATO SE REGULA POR LA LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA, Y EL ARTÍCULO 155 DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO DE SINALOA.*

*LA AFIANZADORA ACEPTA EXPRESAMENTE: CONTINUAR GARANTIZANDO EL CRÉDITO A QUE ESTA PÓLIZA SE REFIERE, AÚN EN EL CASO DE QUE SE OTORGUEN PRÓRROGAS O ESPERA AL DEUDOR, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES QUE SE AFIANZAN; ACEPTA SOMETERSE AL PROCEDIMIENTO DE EJECUCIÓN ESTABLECIDO POR LA LEY FEDERAL DE INSTITUCIONES DE FIANZAS, PARA LA EFECTIVIDAD DE LAS FIANZAS, AÚN PARA EL CASO DE QUE PROCEDIERA EL COBRO DE INTERESES, CON MOTIVO DEL PAGO EXTEMPORÁNEO DEL IMPORTE DE ESTA PÓLIZA DE FIANZA; PARA LA INTERPRETACIÓN Y CUMPLIMIENTO QUE ESTA PÓLIZA REPRESENTA, SE SOMETE A LA JURISDICCIÓN DE LOS TRIBUNALES COMPETENTES DE LA CIUDAD DE CULIACÁN, SIN., RENUNCIANDO PARA ESTE EFECTO A LA QUE PUDIERA CORRESPONDERLE EN RAZÓN DE SU DOMICILIO; ESTA FIANZA PERMANECERÁ EN VIGOR DESDE LA FECHA DE SU EXPEDICIÓN Y DURANTE LA SUBSTANCIACIÓN DE TODOS LOS RECURSOS Y JUICIOS LEGALES QUE SE INTERPONGAN, HASTA QUE SE DICTE **RESOLUCIÓN DEFINITIVA** POR AUTORIDAD COMPETENTE.*

FIRMA DEL REPRESENTANTE AUTORIZADO.



ANEXO NÚM.12

**MODELO DE CONTRATO**

(SE TRATA DE TRANSCRIBIR EL TEXTO ÍNTEGRO DE ESTE FORMATO DE CONTRATO EN PAPEL MEMBRETADO DEL LICITANTE, EN SEÑAL DE QUE ESTÁ DE ACUERDO QUE EN CASO DE RESULTAR ADJUDICADO, ESTE SERÁ TEXTO DEL CONTRATO QUE REGIRÁ)

CONTRATO CERRADO N° **UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**, QUE CELEBRAN POR UNA PARTE LA UNIVERSIDAD AUTÓNOMA DE SINALOA, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "**LA UNIVERSIDAD**" REPRESENTADA POR EL **DR. ROBESPIERRE LIZÁRRAGA OTERO**, DIRECTOR DE ASUNTOS JURÍDICOS. Y POR LA OTRA PARTE \_\_\_\_\_ REPRESENTADA POR EL C. \_\_\_\_\_ A QUIEN EN LO SUCESIVO SE LE DENOMINARA **EL PROVEEDOR**AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLAUSULAS:

**DECLARACIONES**

I. "LA UNIVERSIDAD" **DECLARA QUE:**

- I. QUE CON BASE EN LA LEY ORGÁNICA PROMULGADA EL DIA 7 DE AGOSTO DE 2006, LA UNIVERSIDAD AUTÓNOMA DE SINALOA ES UNA INSTITUCIÓN DE EDUCACIÓN PÚBLICA DESCENTRALIZADA DEL ESTADO, QUE CON BASE AL RÉGIMEN DE LA AUTONOMÍA QUE CONSAGRA LA FRACCIÓN VII DEL ARTÍCULO 30 DE LA CONSTITUCION POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS CUENTA CON PERSONALIDAD JURIDICA PROPIA Y CAPACIDAD PARA ADQUIRIR Y ADMINISTRAR BIENES INTEGRANTES DE SU PATRIMONIO.
- II. TIENE POR FINALIDAD IMPARTIR EDUCACIÓN EN LOS NIVELES MEDIO SUPERIOR, SUBPROFESIONAL, SUPERIOR Y POSGRADO; REALIZAR INVESTIGACIÓN CIENTÍFICA, TECNOLÓGICA Y HUMANISTA; Y CONTRIBUIR AL ESTUDIO, PRESERVACIÓN Y FOMENTO DE LA CULTURA, DIFUNDIENDO AL PUEBLO SUS BENEFICIOS CON ELEVADO PROPÓSITO DE SERVICIO SOCIAL.
- III. EL ORIGEN DE LOS RECURSOS PARA LA ADQUISICIÓN Y/O CONTRATACIÓN DE LOS SERVICIOS DESCRITOS, SON DE PROCEDENCIA ESTATAL PARA EL EJERCICIO FISCAL 2022 DE LA UNIVERSIDAD AUTÓNOMA DE SINALOA.
- IV. EN ATENCIÓN A LO ANTERIOR, "**LA UNIVERSIDAD**" ADJUDICA EL PRESENTE CONTRATO N° **UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA** EN VIRTUD DE CONTAR "EL PROVEEDOR" CON LOS CONOCIMIENTOS Y CAPACIDAD COMPROBADA PARA EL CUMPLIMIENTO DEL PRESENTE INSTRUMENTO JURÍDICO, LLEVÁNDOSE A CABO LA CELEBRACIÓN Y ADJUDICACIÓN DE ESTE DOCUMENTO CON FUNDAMENTO LOS ARTÍCULOS 16 FRACCION II Y III , 23 PRIMER PÁRRAFO, 32 FRACCION I, 33 FRACCION I, 36 FRACCION I Y 37 LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA.
- V. SU REPRESENTANTE, EL DR. **ROBESPIERRE LIZÁRRAGA OTERO**, ACREDITA SU PERSONALIDAD JURÍDICA, EL CUAL CUENTA CON FACULTADES SUFICIENTES PARA OBLIGAR A SU REPRESENTADA EN LOS TÉRMINOS DEL PRESENTE CONVENIO, LAS CUALES NO LE HAN SIDO REVOCADAS, MODIFICADAS O RESTRINGIDAS EN FORMA ALGUNA, SEGÚN NOMBRAMIENTO



EXTENDIDO POR EL **C. DR. JESÚS MADUEÑA MOLINA**, RECTOR TITULAR DE LA UNIVERSIDAD AUTÓNOMA DE SINALOA, EN TÉRMINOS DEL ARTÍCULO 34, FRACCIÓN III DE LA LEY ORGÁNICA DE LA PROPIA INSTITUCIÓN Y EL PODER GENERAL PARA PLEITOS Y COBRANZAS, PODER GENERAL PARA ACTOS DE ADMINISTRACIÓN Y REPRESENTACIÓN LABORAL Y PODER GENERAL PARA PLEITOS Y COBRANZAS EN MATERIA LABORAL, SEGÚN OBRA DE LA ESCRITURA PÚBLICA NÚMERO 6,816, OTORGADO ANTE LA FE DEL **NOTARIO PÚBLICO 162**, CON EJERCICIO Y RESIDENCIA EN EL MUNICIPIO DE CULIACÁN, SINALOA, LICENCIADO **ISMAEL ARENAS ESPINOZA**.

- VI. CUENTA CON EL REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO **UAS651204MZ9** SEÑALA COMO DOMICILIO LEGAL PARA LOS EFECTOS DE ESTE CONTRATO EL UBICADO EN EL CAMPUS RAFAEL BUELNA, BLVD. MIGUEL TAMAYO ESPINOZA DE LOS MONTEROS NO. 2358, DESARROLLO URBANO TRES RÍOS, C.P. 80020, CULIACÁN, SIN.
  
- ii. "EL PROVEEDOR" **DECLARA QUE:**
  - I. LA EMPRESA \_\_\_\_\_, ES UNA PERSONA MORAL, CON REGISTRO FEDERAL DE CONTRIBUYENTES \_\_\_\_\_, CUENTA CON CAPACIDAD JURIDICA PARA CONTRATAR Y OBLIGARSE EN LOS TERMINOS DE ESTE CONTRATO
  - II. SU GIRO CONSISTE ENTRE OTRAS ACTIVIDADES EN: \_\_\_\_\_ CUENTA CON CAPACIDAD TÉCNICA, RECURSOS HUMANOS Y EQUIPO SUFICIENTE PARA VENDER A LA UNIVERSIDAD LOS BIENES OBJETO DE LA PRESENTE LICITACIÓN.
  - III. MANIFIESTA BAJO PROTESTA DE DECIR VERDAD NO ENCONTRARSE EN LOS SUPUESTOS DEL ARTÍCULO 60 DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES PARA EL ESTADO DE SINALOA
  - IV. SEÑALANDO COMO SU DOMICILIO LEGAL PARA EFECTOS DE ESTE CONTRATO EL UBICADO EN: \_\_\_\_\_ . EXPUESTO LO ANTERIOR, LAS PARTES SUJETAN SU COMPROMISO A LA FORMA Y TERMINOS QUE SE ESTABLECEN EN LAS SIGUIENTES CLÁUSULAS:

### CLÁUSULAS

**PRIMERA: OBJETO DEL CONTRATO.-** "LA UNIVERSIDAD" ENCOMIENDA A "EL PROVEEDOR" LA COMPRA DE SERVICIOS QUE ENSEGUIDA SE DETALLAN:

CONS.	CANTIDAD	DESCRIPCION Y CARACTERISTICAS DE LOS BIENES	PRECIO UNITARIO	SUBTOTAL

**SEGUNDA: PRECIOS.-** CON MOTIVO DE LA ADQUISICIÓN DE LOS **SERVICIOS** QUE HAGA LA **UNIVERSIDAD** A EL **PROVEEDOR**, LA **UNIVERSIDAD** LE REALIZARÁ PAGOS MENSUALES, PREVIA ENTREGA DEL **CFDI** CORRESPONDIENTE, DE ACUERDO A LO SIGUIENTE:



LOS PRECIOS SERÁN CONSIDERADOS FIJOS HASTA QUE CONCLUYA LA RELACIÓN CONTRACTUAL, MISMOS QUE INCLUIRÁN TODOS LOS COSTOS INVOLUCRADOS, CONSIDERANDO TOTALMENTE LOS **SERVICIOS** QUE SE REQUIERAN, POR LO QUE **EL PROVEEDOR** NO PODRÁ AGREGAR NINGÚN COSTO EXTRA Y SERÁN INALTERABLES DURANTE LA VIGENCIA DEL PRESENTE CONTRATO.

DE CONFORMIDAD CON LA **LEY**, EL PRESUPUESTO A EJERCER POR ESTE CONCEPTO DURANTE LA VIGENCIA DEL CONTRATO ES DE UN IMPORTE DE \$ \_\_\_\_\_

**TERCERA: FORMA Y LUGAR DE PAGO.-**

LA **UAS**, NO OTORGARÁ ANTICIPO ALGUNO.

LA **UAS** REALIZARÁ EL PAGO DE LOS **CFDI** RESPECTIVOS DE MANERA MENSUAL POR MES VENCIDO CONFORME A LO SIGUIENTE:

PARA REALIZAR EL PAGO CORRESPONDIENTE, **EL PROVEEDOR** DEBERÁ PRESENTAR A MES VENCIDO DE LA PRESTACIÓN DEL **SERVICIOS** SU **CFDI** PARA REVISIÓN A LA DIRECCIÓN DE CONTROL DE BIENES E INVENTARIOS, DURANTE LOS PRIMEROS 10 DÍAS HÁBILES SIGUIENTES AL MES DEL QUE SE ESTÁ FACTURANDO, CON SUS CORRESPONDIENTES NOTAS DE CRÉDITO QUE PROCEDAN, LAS CUALES CONTENDRÁN TODOS LOS DATOS Y REGISTROS REQUERIDOS POR LAS DISPOSICIONES FISCALES APLICABLES; ASIMISMO, EL IMPORTE DEBERÁ CONTEMPLAR LOS DESCUENTOS QUE VOLUNTARIAMENTE SE HAYAN OFRECIDO Y DESGLOSADO EL CONCEPTO DEL IMPUESTO AL VALOR AGREGADO, PARA QUE EL ÁREA REQUERENTE VALIDE EL **CFDI**

**LA UNIVERSIDAD** PAGARÁ DENTRO DE LOS VEINTE DÍAS NATURALES POSTERIORES A LA PRESENTACIÓN DEL **CFDI** RESPECTIVO.

EN CASO DE QUE **EL PROVEEDOR** NO PRESENTE EN TIEMPO Y FORMA LA DOCUMENTACIÓN REQUERIDA PARA EL TRÁMITE DE PAGO, LA FECHA DE PAGO SE CORRERÁ EL MISMO NÚMERO DE DÍAS QUE DURE EL ATRASO.

**CUARTA: ANTICIPO** PARA EFECTOS DE LA PRESENTE LICITACIÓN, NO SE OTORGARÁ ANTICIPO.

**QUINTA: LUGAR DE PRESTACIÓN DE LOS SERVICIOS.-** **EL PROVEEDOR** SE COMPROMETE A REALIZAR LA PRESTACIÓN DEL **SERVICIOS** SOLICITADO, EN LOS DOMICILIOS Y DE CONFORMIDAD CON LO SEÑALADO EN EL ANEXO UNO, DEL PRESENTE CONTRATO.

**SEXTA: VIGENCIA.-** LA VIGENCIA DEL PRESENTE CONTRATO SERÁ A PARTIR DE LA FECHA DE COMUNICACIÓN DEL FALLO Y HASTA EL DÍA \_\_\_\_\_, LA CUAL SERÁ FORZOSA PARA **EL PROVEEDOR** Y VOLUNTARIA PARA **LA UNIVERSIDAD**, CONCLUIDO EL TÉRMINO DEL PRESENTE CONTRATO, NO PODRÁ HABER PRÓRROGA AUTOMÁTICA POR EL SIMPLE TRANSCURSO DEL TIEMPO Y TERMINARÁ SIN NECESIDAD DE DARSE AVISO ENTRE LAS PARTES.

**SEPTIMA: GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.**



**EL PROVEEDOR** DE ACUERDO AL ARTÍCULO 48, CUARTO PÁRRAFO DE LA **LEY**; SE OBLIGA A OTORGAR A **LA UNIVERSIDAD**, A MÁS TARDAR DENTRO DE LOS **DIEZ DÍAS NATURALES** CONTADOS A PARTIR DEL DÍA SIGUIENTE DE LA FECHA DE CELEBRACIÓN Y FIRMA ESTABLECIDA EN ESTE CONTRATO, GARANTÍA DE CUMPLIMIENTO DE TODAS Y CADA UNA DE LAS OBLIGACIONES A SU CARGO DERIVADAS DEL PRESENTE CONTRATO, MEDIANTE FIANZA EXPEDIDA POR COMPAÑÍA AUTORIZADA EN LOS TÉRMINOS DE LA LEY FEDERAL DE INSTITUCIONES DE FIANZAS Y A FAVOR DE **LA UNIVERSIDAD**, POR UN MONTO DEL 10% DEL VALOR MÁXIMO DE ADJUDICACIÓN SIN INCLUIR EL IMPUESTO AL VALOR AGREGADO.

**EL PROVEEDOR** DEBERÁ ENTREGAR DICHA GARANTÍA DE CUMPLIMIENTO DE ESTE CONTRATO DE LA SIGUIENTE FORMA:

**EL PROVEEDOR** DEBERÁ ENTREGAR A **LA UNIVERSIDAD**, GARANTÍA DE CUMPLIMIENTO DEL CONTRATO EN FORMA DE FIANZA OTORGADA POR INSTITUCIÓN AFIANZADORA AUTORIZADA EN LOS TÉRMINOS DE LA LEY FEDERAL DE INSTITUCIONES DE FIANZAS A FAVOR DE **LA UNIVERSIDAD** Y LA FIANZA PERMANECERÁ VIGENTE HASTA **POR UN AÑO** CONTADO A PARTIR DEL DÍA SIGUIENTE AL INCUMPLIMIENTO DEL FIADO, ASI MISMO, DICHA FIANZA ESTARÁ VIGENTE DURANTE LA SUSTANTACIÓN DE TODOS LOS RECURSOS LEGALES O JUICIOS QUE SE INTERPONGAN HASTA QUE SE DICTE LA **RESOLUCIÓN** POR AUTORIDAD COMPETENTE, TAL Y COMO LO ESTABLECE EL PUNTO 15.2 INCISO B, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL DÍA MARTES 8 DE ABRIL DEL AÑO 2003 EN SU PRIMERA SECCIÓN EN LA PÁGINA NÚMERO 75 PARA LAS POLÍTICAS DE OPERACIÓN DE LA **UNIVERSIDAD**.

EN LA PÓLIZA DE FIANZA DEBERÁ ASENTARSE LO SIGUIENTE:

- A) QUE SE OTORGA PARA GARANTIZAR TODAS Y CADA UNA DE LAS OBLIGACIONES CONTENIDAS EN EL **CONTRATO No. \_\_\_\_\_** DE FECHA \_\_\_\_\_ **DE 2022** CELEBRADO ENTRE **EL PROVEEDOR Y LA UNIVERSIDAD**, DERIVADOS DEL PROCESO DE **LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA**.
- B) EN CASO DE QUE LA PRESENTE FIANZA SE HAGA EXIGIBLE LA AFIANZADORA ADMITE EXPRESAMENTE SOMETERSE INDISTINTAMENTE Y A ELECCIÓN DEL BENEFICIARIO A CUALQUIERA DE LOS PROCEDIMIENTOS LEGALES ESTABLECIDOS EN LOS ARTÍCULOS 93 Y/O 94 DE LA LEY DE INSTITUCIONES DE FIANZAS, O BIEN A TRAVÉS DEL ART. 63 DE LA LEY DE PROTECCIÓN Y DEFENSA AL USUARIO DE SERVICIOS FINANCIEROS.
- c) ESTA FIANZA CONTINUARA VIGENTE AUN CUANDO SE OTORGUEN PRORROGAS O ESPERAS AL PRESTADOR DEL **SERVICIOS**, PARA EL CUMPLIMIENTO DE SUS OBLIGACIONES QUE SE AFIANZAN.
- d) LA PRESENTE FIANZA PERMANECERÁ EN VIGOR DESDE LA FECHA DE SU EXPEDICIÓN Y HASTA EL CUMPLIMIENTO TOTAL DE LA PRESTACIÓN DE LOS **SERVICIOS** OFERTADOS EN EL **ANEXO UNO**, POR PARTE DE **EL PROVEEDOR** DE LA AFIANZADORA, O EN SU CASO



DURANTE LA SUBSTANCIACIÓN DE TODOS LOS RECURSOS LEGALES O JUICIOS QUE SE INTERPONGAN, HASTA QUE SE DICTE LA **RESOLUCIÓN** DEFINITIVA POR AUTORIDAD COMPETENTE.

- e) PARA LA CANCELACIÓN DE LA FIANZA, SERÁ REQUISITO INDISPENSABLE LA CONFORMIDAD EXPRESA Y POR ESCRITO DE LA **UNIVERSIDAD** AUTONOMA DE SINALOA..

**OCTAVA: OBLIGACIONES.- EL PROVEEDOR** OBLIGA A PLANEAR, PROGRAMAR, DIRIGIR Y EJECUTAR EN FORMA PERMANENTE LAS ACCIONES **NECESARIAS** PARA LLEVAR A CABO LA PRESTACIÓN **DE LOS SERVICIOS** A QUE SE REFIERE LA CLAUSULA PRIMERA DE ESTE CONTRATO, A FIN DE CUMPLIR EN FORMA EFICAZ Y OPORTUNA CON LO SOLICITADO.

ENTREGAR EN TIEMPO Y FORMA LOS **SERVICIOS** REQUERIDOS POR **LA UNIVERSIDAD**, DE ACUERDO A LOS PEDIDOS QUE EN SU CASO FINCADOS.

INSTRUIR A SU PERSONAL PARA QUE EN LA PRESTACIÓN DE LOS **SERVICIOS** RESPETE LAS DISPOSICIONES DE ORDEN Y DISCIPLINA QUE RIGEN EN **LA UNIVERSIDAD**.

**NOVENA. CALIDAD.- CALIDAD.- EL PROVEEDOR** DEBERA CONTAR CON LA INFRAESTRUCTURA NECESARIA, PERSONAL TECNICO ESPECIALIZADO EN EL RAMO, PROCEDIMIENTOS, TECNICAS Y EQUIPOS ADECUADOS, A FIN DE GARANTIZAR QUE LOS **SERVICIOS** OBJETO DE ESTE CONTRATO SEAN PROPORCIONADOS CON LA CALIDAD, OPORTUNIDAD Y EFICIENCIA REQUERIDA, COMPROMETIENDOSE A DESARROLLARLO A ENTERA SATISFACCION DE LA **UNIVERSIDAD**.

PERSONAL AUTORIZADO DE LA **UNIVERSIDAD** SUPERVISARA LA REALIZACIÓN CORRECTA Y EFICIENTE DE LOS **SERVICIOS** OBJETO DE ESTE CONTRATO.

**DECIMA. RELACION LABORAL.-** LAS PARTES CONVIENEN EN QUE **LA UNIVERSIDAD** NO ADQUIERE NINGUNA OBLIGACION CON **EL PROVEEDOR** DE CARACTER LABORAL, NI CON LOS TRABAJADORES QUE EL MISMO CONTRATE PARA LA ENTREGA DE LOS **SERVICIOS** OBJETO DEL PRESENTE INSTRUMENTO JURIDICO, POR LO QUE A **LA UNIVERSIDAD** NO SE LE CONSIDERARA COMO PATRÓN, NI AUN SUBSTITUTO Y **EL PROVEEDOR** EXPRESAMENTE LO EXIME DE CUALQUIER RESPONSABILIDAD DE CARACTER CIVIL, PENAL, LABORAL, FISCAL, DE SEGURIDAD SOCIAL O DE CUALQUIER OTRA INDOLE QUE EN SU CASO PUDIERA LLEGAR A PRESENTARSE.

**EL PROVEEDOR** SERA RESPONSABLE SOLIDARIO POR LA NEGLIGENCIA, IMPERICIA O DOLO EN QUE INCURRAN LOS TRABAJADORES A SU **SERVICIOS**, DE CONFORMIDAD CON LO DISPUESTO EN EL ARTICULO 1924 DEL CODIGO CIVIL FEDERAL.

**DECIMA PRIMERA: PENA CONVENCIONAL.-** EN CASO DE ATRASO EN EL CUMPLIMIENTO EN LA PRESTACIÓN DE LOS **SERVICIOS**, POR CAUSAS IMPUTABLES AL PROVEEDOR, ESTE QUEDARÁ OBLIGADO A PAGAR POR CONCEPTO DE PENA CONVENCIONAL, EL 0.1%, POR CADA DÍA NATURAL DE ATRASO EN LA PRESTACIÓN DE LOS **SERVICIOS**, SOBRE EL IMPORTE TOTAL DEL CONTRATO MENSUAL DE LA TARIFA UNITARIA DEL **SERVICIOS** RELACIONADO CON EL INCUMPLIMIENTO, POR CADA DIA NATURAL DE





ATRASO EN LA ENTREGA DE LOS **SERVICIOS**, HASTA SU CUMPLIMIENTO A ENTERA SATISFACCIÓN DE **LA UNIVERSIDAD**., PROCEDIENDO ESTE ULTIMO A EFECTUAR EL DESCUENTO DIRECTO DEL ENTERO DE LA FACTURACION QUE DEBA CUBRIR DEBIENDO **EL PROVEEDOR** ENTREGAR UNA NOTA DE CREDITO QUE SE APLICARA EN LA FACTURACION CORRESPONDIENTE.

SI EN UN TERMINO DE 10 DIAS NATURALES PERSISTE EL ATRASO, **LA UNIVERSIDAD** PODRA RESCINDIR ADMINISTRATIVAMENTE EL CONTRATO Y EN SU CASO HARA EFECTIVA LA FIANZA DE GARANTIA DEL CUMPLIMIENTO.

LA PENA CONVENCIONAL A CARGO **DEL PROVEEDOR** POR NINGUN CONCEPTO PODRA EXCEDER EL MONTO DE LA GARANTIA DEL CUMPLIMIENTO DEL CONTRATO

**DECIMA SEGUNDA. SANCIONES.-** CON FUNDAMENTO EN EL PRIMER PÁRRAFO DE ARTÍCULO 82 DE LA **LEY**, LA CONTRALORIA SANCIONARÁ A **EL PROVEEDOR** CUANDO INFRINJA LAS DISPOSICIONES DE LA **LEY**, CON MULTA EQUIVALENTE A LA CANTIDAD DE CINCUENTA HASTA MIL VECES EL SALARIO MÍNIMO GENERAL VIGENTE EN EL ESTADO DE SINALOA ELEVADO AL MES, EN LA FECHA DE LA INFRACCIÓN.

- A) QUE INJUSTIFICADAMENTE Y POR CAUSAS IMPUTABLES A LOS MISMOS NO FORMALICEN EL CONTRATO ADJUDICADO POR **LA UNIVERSIDAD**.
- B) QUE SE ENCUENTREN EN EL SUPUESTO DE ARTÍCULOS 60 Y 83 DE **LA LEY**.
- C) QUE NO CUMPLA CON SUS OBLIGACIONES CONTRACTUALES POR CAUSAS IMPUTABLES A EL Y QUE, COMO CONSECUENCIA, CAUSEN DAÑOS O PERJUICIOS GRAVES A **LA UNIVERSIDAD**, ASI COMO CUANDO ENTREGUE BIENES CON ESPECIFICACIONES DISTINTAS DE LAS CONVENIDAS, Y
- D) QUE PROPORCIONE INFORMACION FALSA O QUE ACTUEN CON DOLO O MALA FE EN ALGUN PROCEDIMIENTO DE CONTRATACION, EN LA CELEBRACION DEL CONTRATO O DURANTE SU VIGENCIA O BIEN EN LA PRESENTACION O DESAHOGO DE UNA QUEJA EN UNA AUDIENCIA DE CONCILIACION O DE UNA INCONFORMIDAD.

**DECIMA TERCERA: IMPUESTOS Y DERECHOS.-** LOS IMPUESTOS Y DERECHOS QUE PROCEDAN CON MOTIVO DE LA CONTRATACION DE LOS **SERVICIOS** OBJETO DEL PRESENTE INSTRUMENTO JURIDICO, SERAN PAGADOS POR **EL PROVEEDOR**.

**LA UNIVERSIDAD** SOLO CUBRIRA EL IMPUESTO AL VALOR AGREGADO, DE ACUERDO A LO ESTABLECIDO EN LAS DISPOSICIONES LEGALES VIGENTES EN LA MATERIA.

**DECIMA CUARTA: PATENTES Y MARCAS.-** **EL PROVEEDOR** SERA RESPONSABLE EN CASO DE QUE CON LA ENTREGA DE **SERVICIOS**, INFRINJA PATENTES Y/O MARCAS REGISTRADAS DE TERCEROS, QUEDANDO OBLIGADO A LIBERAR A **LA UNIVERSIDAD** DE TODA RESPONSABILIDAD DE CARACTER CIVIL, PENAL, MERCANTIL, FISCAL O DE CUALQUIER OTRA INDOLE

**DECIMA QUINTA: PROHIBICION DE CESION DE DERECHOS Y OBLIGACIONES.-** **EL PROVEEDOR** NO PODRA TRANSMITIR BAJO NINGUN TITULO, LOS DERECHOS Y OBLIGACIONES QUE SE ESTABLEZCAN EN EL PRESENTE CONTRATO, CON EXCEPCION DE LOS DERECHOS DE COBRO, EN CUYO CASO SE DEBERA CONTAR CON LA CONFORMIDAD PREVIA DE **LA UNIVERSIDAD**.



IGUALMENTE, BAJO NINGUNA CIRCUNSTANCIA PODRAN SER NEGOCIADAS LAS CONDICIONES ESTIPULADAS EN EL PRESENTE INSTRUMENTO JURIDICO.

**DECIMA SEXTA: RESCISION Y TERMINACION ANTICIPADA.- LA UNIVERSIDAD** PODRA RESCINDIR ADMINISTRATIVAMENTE ESTE CONTRATO EN CASO DE CUALQUIER INCUMPLIMIENTO A LAS CONDICIONES ESTABLECIDAS EN EL MISMO, SIN NECESIDAD DE ACUDIR A LOS TRIBUNALES COMPETENTES EN LA MATERIA, EN CUYO CASO EL PROCEDIMIENTO DEBERA INICIARSE DENTRO DE LOS QUINCE DIAS NATURALES SIGUIENTES A AQUEL EN QUE SE HUBIERE AGOTADO EL MONTO LIMITE DE APLICACION DE LAS PENAS CONVENCIONALES. SI PREVIAMENTE A LA DETERMINACION DE DAR POR RESCINDIDO EL CONTRATO SE ENTREGAREN LA TOTALIDAD DE LOS **SERVICIOS**, EL PROCEDIMIENTO INICIADO QUEDARA SIN EFECTO. POR LO QUE DE MANERA ENUNCIATIVA, MAS NO LIMITATIVA, SE ENTENDERA POR INCUMPLIMIENTO:

- A) SI **EL PROVEEDOR**NO REALIZA LA PRESTACIÓN DE LOS **SERVICIOS** OBJETO DE ESTE CONTRATO CON LA CALIDAD, EFICIENCIA Y ESPECIFICACIONES SOLICITADAS POR **LA UNIVERSIDAD**.
- B) CUANDO **EL PROVEEDOR**CEDA TOTAL O PARCIALMENTE, BAJO CUALQUIER TITULO, LOS DERECHOS Y OBLIGACIONES A QUE SE REFIERA EL CONTRATO.
- C) QUE **EL PROVEEDOR** NO CUMPLA EN TIEMPO Y FORMA CON LA ENTREGA DE LOS **SERVICIOS** CONFORME A LO ESTABLECIDO POR **LA UNIVERSIDAD**.
- D) CUANDO LA AUTORIDAD COMPETENTE DECLARE EL ESTADO DE QUIEBRA, LA SUSPENSION DE PAGOS O ALGUNA SITUACION DISTINTA, QUE SEA ANALOGA O EQUIVALENTE Y QUE AFECTE EL PATRIMONIO DE **EL PROVEEDOR**.
- E) SI TRANSCURRIDO EL PLAZO SEÑALADO EN EL ARTICULO 48 PARRAFO SEGUNDO DE LA LEY **EL PROVEEDOR**NO HA PRESENTADO LA GARANTIA DE CUMPLIMIENTO.
- F) EN GENERAL, INCURRA EN INCUMPLIMIENTO TOTAL O PARCIAL DE LAS OBLIGACIONES QUE SE ESTIPULEN EN ESTE CONTRATO.

PARA EL CASO DE OPTAR POR LA RESCISION DEL CONTRATO, LA **UNIVERSIDAD** COMUNICARA POR ESCRITO AL PROVEEDOR EL INCUMPLIMIENTO EN QUE HAYA INCURRIDO, PARA QUE EN UN TERMINO DE DIEZ DIAS HABILES EXPONGA LO QUE A SU DERECHO CONVenga Y APORTE LAS PRUEBAS QUE ESTIME PERTINENTES, TRANSCURRIDO DICHO TERMINO SE RESOLVERA CONSIDERANDO LOS ARGUMENTOS Y PRUEBAS QUE SE HUBIEREN HECHO VALER, DEBIENDO FUNDAR Y MOTIVAR DEBIDAMENTE LA RESOLUCION Y LO COMUNICARA POR ESCRITO AL PROVEEDOR DENTRO DEL TERMINO SEÑALADO POR LA FRACCION III DEL ARTICULO 54 DE LA LEY.

CUANDO SE PRESENTE CUALQUIERA DE LOS CASOS MENCIONADOS, **LA UNIVERSIDAD** QUEDARA EXPRESAMENTE FACULTADO PARA OPTAR POR EXIGIR EL CUMPLIMIENTO DEL CONTRATO, APLICANDO LAS PENAS CONVENCIONALES Y/O RESCINDIRLO, SIENDO ESTA SITUACION UNA FACULTAD POTESTATIVA.





ASIMISMO, **LA UNIVERSIDAD** PODRA DAR POR TERMINADO ANTICIPADAMENTE EL CONTRATO, CUANDO CONCURRAN RAZONES DE INTERES GENERAL O BIEN, CUANDO POR CAUSAS JUSTIFICADAS SE EXTINGA LA NECESIDAD DE REQUERIR LOS **SERVICIOS** ORIGINALMENTE CONTRATADOS.

**DECIMA SÉPTIMA: JURISDICCION.-** EN CASO DE CONTROVERSIAS QUE SE SUSCITEN CON MOTIVO DE LA INTERPRETACIÓN, CUMPLIMIENTO Y EJECUCIÓN DEL PRESENTE CONTRATO, LAS PARTES SE SOMETEN A LA JURISDICCIÓN DE LOS TRIBUNALES COMPETENTES DE LA CIUDAD DE CULIACÁN, SIN., RENUNCIANDO AL FUERO QUE PUDIERA CORRESPONDERLES POR RAZÓN DE SU DOMICILIO PRESENTE O FUTURO, O CUALQUIER OTRA CAUSA.

LEIDO QUE FUE Y ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DEL PRESENTE CONTRATO, LO FIRMAN AL MARGEN Y AL CALCE POR TRIPLICADO, EN LA CIUDAD DE CULIACÁN, SINALOA, EL DIA \_\_\_\_\_.

**POR "LA UNIVERSIDAD**

**POR "EL PROVEEDOR"**

**DR. ROBESPIERRE LIZÁRRAGA OTERO**  
**DIRECTOR DE ASUNTOS JURIDICOS**

LAS FIRMAS QUE ANTECEDEN CORRESPONDEN AL CONTRATO CERRADO \_\_\_\_\_ QUE CELEBRAN POR UNA PARTE LA UNIVERSIDAD AUTÓNOMA DE SINALOA, Y POR LA OTRA PARTE -----



---

**ANEXO NÚM. 13**

**UTILIZAR PAPEL MEMBRETADO DEL LICITANTE**

**CARTA-RESPALDO DEL FABRICANTE O DISTRIBUIDOR AUTORIZADO DE LOS SERVICIOS**

LUGAR Y FECHA

**M.C. SALVADOR PÉREZ MARTÍNEZ**

PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

**“INDICAR NOMBRE DEL REPRESENTANTE O APODERADO LEGAL DEL FABRICANTE O DISTRIBUIDOR AUTORIZADO”, EN MI CARÁCTER DE REPRESENTANTE O APODERADO LEGAL DE (FABRICANTE O DISTRIBUIDOR AUTORIZADO), Y CON RELACIÓN A LA LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA, MANIFIESTO BAJO PROTESTA DE DECIR VERDAD, NUESTRO APOYO SOLIDARIO CON LA EMPRESA “INDICAR LA RAZON SOCIAL DEL LICITANTE”, PARA CUMPLIR CONJUNTAMENTE CON LOS COMPROMISOS DE ENTREGA DE LA INFRAESTRUCTURA EMPLEADA PARA LA PRESTACIÓN DE LOS SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA”, QUE LE SEAN ADJUDICADOS.**

POR LO ANTERIOR, LA INFRAESTRUCTURA EMPLEADA PARA LA PRESTACIÓN DE LOS **SERVICIOS** ANTES CITADOS, SERA BAJO LOS REQUERIMIENTOS SOLICITADOS POR **LA UNIVERSIDAD** Y SERAN SUMINISTRADOS EN TIEMPO Y FORMA A LA EMPRESA **“INDICAR RAZON SOCIAL DEL LICITANTE”** PARA QUE ESTA A SU VEZ, REALICE LA IMPLEMENTACIÓN DE LA MISMA Y ESTE EN CONDICIONES DE BRINDAR LOS **SERVICIOS A LA UNIVERSIDAD** EN EL LUGAR Y FOMA, INDICADOS EN LA CONVOCATORIA DEL PROCESO DE CONTRATACIÓN.

LO ANTERIOR, ES CON LA FINALIDAD DE DAR CUMPLIMIENTO A LAS DISPOSICIONES LEGALES QUE CORRESPONDAN Y A LA CONVOCATORIA Y ANEXOS DEL PROCESO DE CONTRATACION DE REFERENCIA.

---

**NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL  
DEL FABRICANTE O DISTRIBUIDOR AUTORIZADO.**



**ANEXO NÚM. 14**

UTILIZAR PAPEL MEMBRETADO DEL LICITANTE

**(MODELO DE ESCRITO PARA ACLARACIÓN DE DUDAS DE LA CONVOCATORIA)**

LUGAR Y FECHA

**M.C. SALVADOR PÉREZ MARTÍNEZ**  
PRESIDENTE DEL COMITÉ DE ADQUISICIONES Y  
SECRETARIO DE ADMINISTRACIÓN Y FINANZAS  
P R E S E N T E.-

YO \_\_\_\_\_ CON RELACIÓN A LA LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA, EN MI CALIDAD DE LICITANTE, SOLICITO A USTED MUY ATENTAMENTE ACLARARNOS LAS SIGUIENTES DUDAS:

**PREGUNTA # 1**

	NUMERO DE PAGINA	DE	NUMERAL DE CONTENIDO	PARRAFO
DUDA OBSERVACION:	U			
RESPUESTA:				

**Pregunta #2**

	NUMERO DE PAGINA	DE	NUMERAL DE CONTENIDO	PARRAFO
DUDA OBSERVACION:	U			
RESPUESTA:				

**Pregunta #3**

<b>DUDA U OBSERVACION GENÉRICA: (Cualquier pregunta sin relación a determinado inciso)</b>				
DUDA OBSERVACION:	U			
RESPUESTA:				



**ANEXO NÚM. 15**

LISTADO DE VERIFICACIÓN DE LOS REQUISITOS DOCUMENTALES QUE DEBEN PRESENTAR LOS LICITANTES EN ACTO DE RECEPCION Y APERTURA DE LAS PROPUESTAS DE LA LICITACIÓN PÚBLICA NACIONAL NÚM. LPN-UAS-01-2022 SERVICIOS ADMINISTRADOS DE SEGURIDAD INFORMÁTICA

**VERIFICACION-ACUSE DE RECIBIDO**

<b>NOMBRE DE LA EMPRESA :</b>			
<b>NOMBRE DEL REPRESENTANTE LEGAL:</b>			
NUMERAL	DESCRIPCIÓN	CUMPLE	
		SI	NO
<b>RELACIÓN DE DOCUMENTOS SOLICITADOS EN EL PUNTO 5.1 DE ESTAS BASES DOCUMENTACIÓN LEGAL Y ADMINISTRATIVA</b>			
<b>PUNTO 5.1.a)</b>	ORIGINAL Y COPIA LEGIBLE DE IDENTIFICACIÓN OFICIAL VIGENTE DE EL LICITANTE, O SU REPRESENTANTE LEGAL, (CREDENCIAL PARA VOTAR CON FOTOGRAFÍA, CARTILLA DEL SERVICIO MILITAR NACIONAL, CÉDULA PROFESIONAL O PASAPORTE).		
<b>PUNTO 5.1.b)</b>	CONSTANCIA DE SITUACIÓN FISCAL CON ANTIGÜEDAD NO MAYOR A 3 MESES		
<b>PUNTO 5.1.c)</b>	COMPROBANTE DE DOMICILIO (RECIBO DE CFE, AGUA, TELÉFONO) CON ANTIGÜEDAD NO MAYOR A 3 MESES.		
<b>PUNTO 5.1.d)</b>	OPINIÓN DE CUMPLIMIENTO VIGENTE EN SENTIDO POSITIVO, RESPECTO AL CUMPLIMIENTO DE OBLIGACIONES FISCALES, EXPEDIDO POR EL SAT, A FAVOR DEL LICITANTE. CON ANTIGÜEDAD NO MAYOR A 1 MES.		
<b>PUNTO 5.1.e)</b>	OPINIÓN DE CUMPLIMIENTO VIGENTE EN SENTIDO POSITIVO, RESPECTO AL CUMPLIMIENTO DE OBLIGACIONES EN MATERIA DE SEGURIDAD SOCIAL, EXPEDIDO POR EL IMSS, A FAVOR DEL LICITANTE.		
<b>PUNTO 5.1.f)</b>	CONSTANCIA DE SITUACIÓN FISCAL VIGENTE DE NO ADEUDOS DE VIGENCIA, EXPEDIDO POR EL INFONAVIT A FAVOR DEL LICITANTE.		
<b>PUNTO 5.1.g)</b>	ORIGINAL DE CARTA PODER SIMPLE CONFORME AL ANEXO NÚM. 4 (EN CASO QUE APLIQUE)		
<b>PUNTO 5.1.h)</b>	ESCRITO CONFORME AL ANEXO NÚM. 5 DONDE EL LICITANTE MANIFIESTE QUE HA TENIDO DEBIDO CONOCIMIENTO DEL CONTENIDO DE LA CONVOCATORIA		
<b>PUNTO 5.1.i)</b>	DECLARACIÓN ESCRITA, CONFORME AL ANEXO NÚM. 6, DONDE MANIFIESTE BAJO PROTESTA DE DECIR VERDAD, DE NO ENCONTRARSE EN ALGUNO DE LOS SUPUESTOS ESTABLECIDOS POR LOS ARTÍCULOS 50 Y 60 PENÚLTIMO PÁRRAFO, DE LA LEY		
<b>PUNTO 5.1.j)</b>	DECLARACIÓN DE INTEGRIDAD, CONFORME AL ANEXO NÚM. 7.		
<b>PUNTO 5.1.k)</b>	CONVENIO DE PARTICIPACIÓN CONJUNTA (UNICAMENTE SI APLICA)		
<b>RELACIÓN DE DOCUMENTOS SOLICITADOS EN EL PUNTO 5.2 DE ESTAS BASES PROPUESTA TÉCNICA</b>			



<b>PUNTO 5.2.a)</b>	LOS <b>LICITANTES</b> DEBERÁN DESCRIBIR DETALLADA Y ESPECÍFICAMENTE LOS <b>SERVICIOS</b> OFERTADOS, CONTENIDOS EN EL NUMERAL 2.1 Y EL <b>ANEXO A</b> , DEBIENDO UTILIZAR EL <b>ANEXO NÚM. 1</b> , PARA SU PROPUESTA TÉCNICA.  COMO PARTE INTEGRANTE DE SU PROPUESTA, <b>LOS LICITANTES</b> DEBERÁN PRESENTAR <b>FOLLETOS Y/O CATÁLOGOS</b> DE LAS HERRAMIENTAS PROPUESTAS, ÉSTOS DEBERÁN SER NUEVOS Y SIN ANUNCIO DE FIN DE VIDA, DE ACUERDO A LAS ESPECIFICACIONES DEL ANEXO I DEL PUNTO 1 DE LA PRESENTE CONVOCATORIA		
<b>PUNTO 5.2.b)</b>	ESCRITO ORIGINAL FIRMADO POR EL REPRESENTANTE LEGAL DONDE PRECISE LA GARANTÍA DE LA INFRAESTRUCTURA CONTRA DEFECTOS DE FABRICACIÓN Y/O VICIOS OCULTOS, CONFORME A LO SOLICITADO <b>PUNTO 2.3</b> UTILIZANDO EL FORMATO CONTENIDO EN EL <b>ANEXO NÚM. 8</b> .		
<b>PUNTO 5.2.c)</b>	ESCRITO ORIGINAL FIRMADO POR EL REPRESENTANTE LEGAL DONDE SE COMPROMETA <b>EL LICITANTE</b> QUE EN CASO DE QUE SE LE ADJUDIQUE EL CONTRATO ASUMIRÁ LA RESPONSABILIDAD TOTAL EN CASO DE QUE INFRINJA PATENTES, MARCAS REGISTRADAS O VIOLE DERECHOS EXCLUSIVOS DE AUTOR O PROPIEDAD INDUSTRIAL, UTILIZANDO COMO MODELO EL <b>(ANEXO NÚM. 9)</b> .		
<b>PUNTO 5.2.d)</b>	EN EL CASO DE LAS <b>MIPYMES</b> PODRÁN PARTICIPAR CON ESE CARÁCTER, UTILIZANDO PARA TAL FIN EL FORMATO QUE SE ACOMPAÑA COMO <b>(ANEXO NÚM. 10)</b> .		
<b>PUNTO 5.2.e)</b>	ESCRITO ORIGINAL FIRMADO POR EL REPRESENTANTE LEGAL DONDE TRANSCRIBA <b>EL LICITANTE</b> EL FORMATO DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO		
<b>PUNTO 5.2.g)</b>	ESCRITO ORIGINAL FIRMADO POR EL REPRESENTANTE LEGAL, DE CONFORMIDAD CON EL <b>PUNTO 2.7</b> DE LAS BASES EN EL CUAL TRANSCRIBA EN PAPEL MEMBRETADO DEL <b>LICITANTE</b> , EL <b>FORMATO DE CONTRATO</b> QUE SERÍA UTILIZADO EN CASO DE RESULTAR ADJUDICADO, UTILIZANDO EL FORMATO CONTENIDO EN EL <b>ANEXO NÚM. 13</b> DE ESTAS BASES		
<b>5.2.h)</b>	ARCHIVO ELECTRÓNICO (EN USB) DE TODA LA DOCUMENTACION QUE INTEGRA LA PROPOSICION		



5.2.i)	<p>a) LOS PARTICIPANTES DEBERÁN CONTAR CON UN SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DENTRO DEL TERRITORIO NACIONAL, LO CUAL DEBERA ACREDITAR CON LOS SIGUIENTES CERTIFICADOS VIGENTES A NOMBRE DEL LICITANTE.</p> <ul style="list-style-type: none"><li>i. LA NORMA INTERNACIONAL UNE-ISO/IEC 27001:2014 (RELATIVA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN)</li><li>ii. LA NORMA INTERNACIONAL UNE-ISO/IEC 20000-1:2018 (RELATIVA AL SISTEMA DE GESTIÓN DE TI)</li><li>iii. LA NORMA INTERNACIONAL UNE-EN ISO 22301:2015 (RELATIVA AL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO)</li></ul> <p>LOS PARTICIPANTES DEBERAN INCLUIR DENTRO DE SU PROPUESTA TECNICA, COPIA SIMPLE DE LOS CERTIFICADOS ANTES MENCIONADOS.</p>		
<b>PUNTO</b> 5.2.j)	ESCRITO ORIGINAL FIRMADO POR EL REPRESENTANTE LEGAL, EN EL CUAL TRANSCRIBA EN PAPEL MEMBRETADO DEL LICITANTE, EL FORMATO DE <b>CARTA-RESPALDO DEL FABRICANTE O DISTRIBUIDOR</b> AUTORIZADO DE LOS <b>SERVICIOS</b> , UTILIZANDO EL FORMATO CONTENIDO EN EL <b>ANEXO NÚM. 13</b> DE ESTAS BASES		



<p><b>PUNTO</b> <b>5.2.g)</b></p>	<p>LOS PARTICIPANTES DEBERÁN CONTAR CON UN SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DENTRO DEL TERRITORIO NACIONAL, LO CUAL DEBERA ACREDITAR CON LOS SIGUIENTES CERTIFICADOS VIGENTES A NOMBRE DEL <b>LICITANTE</b>.</p> <ul style="list-style-type: none"> <li>i. LA NORMA INTERNACIONAL UNE-ISO/IEC 27001:2014 (RELATIVA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN)</li> <li>ii. LA NORMA INTERNACIONAL UNE-ISO/IEC 20000-1:2018 (RELATIVA AL SISTEMA DE GESTIÓN DE TI)</li> <li>iii. LA NORMA INTERNACIONAL UNE-EN ISO 22301:2015 (RELATIVA AL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO)</li> </ul> <p>LOS PARTICIPANTES DEBERAN INCLUIR DENTRO DE SU PROPUESTA TECNICA, COPIA SIMPLE DE LOS CERTIFICADOS ANTES MENCIONADOS.</p>		
<p><b>PUNTO</b> <b>5.2.h)</b></p>	<p>ARCHIVO ELECTRÓNICO EN <b>USB</b>, QUE CONTENGA TODA LA INFORMACIÓN QUE PRESENTA EN SUS PROPUESTAS PARA CUMPLIR CON LOS NUMERALES 5.1, 5.2 Y 5.3</p>		
<p><b>PUNTO</b> <b>5.2.i)</b></p>	<p>LOS PARTICIPANTES DEBERÁN PRESENTAR <b>FOLLETOS Y/O CATÁLOGOS</b> DE LAS HERRAMIENTAS PROPUESTAS, ÉSTOS DEBERÁN SER NUEVOS Y SIN ANUNCIO DE FIN DE VIDA, DE ACUERDO A LAS ESPECIFICACIONES DEL ANEXO I DEL PUNTO 1 DE LA PRESENTE CONVOCATORIA</p>		
<p><b>PUNTO</b> <b>5.2.j)</b></p>	<p>LOS PARTICIPANTES DEBERÁN ACREDITAR CONTAR CON UN SOC (CENTRO DE OPERACIONES DE SEGURIDAD) DENTRO DEL TERRITORIO NACIONAL, EL CUAL DEBERA CONTAR CON LOS SIGUIENTES CERTIFICADOS VIGENTES.</p> <ul style="list-style-type: none"> <li>i. LA NORMA INTERNACIONAL ISO27001 (RELATIVA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN)</li> <li>ii. LA NORMA INTERNACIONAL ISO20000 (RELATIVA AL SISTEMA DE GESTIÓN DE TI)</li> <li>iii. LA NORMA INTERNACIONAL ISO22301 (RELATIVA AL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO)</li> </ul>		
<p><b>RELACIÓN DE DOCUMENTOS SOLICITADOS EN EL PUNTO 5.3 DE ESTAS BASES</b> <b>PROPUESTA ECONÓMICA</b></p>			
<p><b>PUNTO</b> <b>5.3.a)</b></p>	<p><b>ANEXO No. 2, PROPUESTA ECONÓMICA</b></p>		

**A ELECCIÓN DEL LICITANTE, LA DOCUMENTACIÓN RELACIONADA EN LOS PUNTOS 5.1 PODRÁ ENTREGARSE DENTRO O FUERA DEL SOBRE QUE CONTENGA LA PROPUESTA TÉCNICA.**

**RECIBE POR PARTE DE LA UNIVERSIDAD**

(EL PRESENTE FORMATO, SERVIRÁ ÚNICAMENTE COMO GUÍA PARA LA INTEGRACION Y RECEPCIÓN DE LA DOCUMENTACIÓN SOLICITADA; EL HECHO QUE EL LICITANTE HAYA ENTREGADO TODA SU DOCUMENTACIÓN, NO IMPLICA EL CUMPLIMIENTO DEL MISMO.)