

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

REF.: ELABORACIÓN DE ESPECIFICACIONES
TÉCNICAS PARA LA "ADQUISICIÓN DE DISPOSITIVOS
DE SEGURIDAD Y RENOVACIÓN DE LICENCIAS DE
SISTEMA DE PROTECCIÓN PARA EL DATACENTER DE
LA JUSTICIA ELECTORAL".

DICTAMEN TÉCNICO DTIC N° 03/2024

Asunción, 13 de junio de 2.024

I) INTRODUCCIÓN

El Director de la Dirección de Tecnologías de la Información y Comunicación, Lic. Fausto Von Streber, a fin de dar cumplimiento a lo establecido en el Art. 40 –Documentaciones - de la Resolución DNCP N° 4401/2023, modificado por el Art. 12 de la Resolución DNCP N° 453/2024, procedo a elevar el presente dictamen técnico referente a la elaboración de las especificaciones técnicas tendientes a la realización de un procedimiento de contratación pública para la "Adquisición de Dispositivos de Seguridad y Renovación de Licencias de Sistema de Protección para el Datacenter de la Justicia Electoral", en los términos que paso a exponer a continuación:

II) MARCO NORMATIVO Y PARECER TÉCNICO

El Artículo 25°, primer apartado de la Ley N° 7021/2022 "DE SUMINISTRO Y CONTRATACIONES PÚBLICAS" dispone: "Para iniciar el procedimiento de contratación, la convocante deberá especificar al nivel más detallado posible los bienes, servicios, consultorías y obras públicas a adquirir con el fin de satisfacer sus necesidades...".

El Artículo 40° del Decreto N° 9823/2023 "Por el cual se reglamenta la Ley N° 7021/2022 «DE SUMINISTRO Y CONTRATACIONES PÚBLICAS»" reza: "Las especificaciones técnicas que deban contener las bases de la contratación, se establecerán con la mayor amplitud de acuerdo con la naturaleza específica del contrato, con el objeto de que concurra el mayor número de oferentes...".

El Artículo 40° de la Resolución DNCP N° 4401/23, modificado por el Art. 12 de la Resolución DNCP N° 453/24, el cual dispone: "La comunicación que realice la convocante a la DNCP a través del SICP, a los efectos de la verificación y la difusión de los procedimientos de contratación, además del pliego de bases y condiciones particular, deberá remitir mínimamente la siguiente documentación: a) Dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, refrendado por el responsable del área requirente o del técnico que las recomendó...".

Lo dispuesto por la Circular de la Dirección Nacional de Contrataciones Públicas N° 27/2024, que establece las Directrices o Modelo de Dictamen Técnico (Art.° 40 inc. a) Res. DNCP N° 4401 y Res DNCP N° 453 Art.° 12, en base a la cual se exponen los ítems y fundamentos conforme al siguiente detalle:

UOC Convocante: Justicia Electoral

Unidad o área requirente: Dirección de Tecnologías de la Información y Comunicación

Funcionario o técnico responsable: Lic. Fausto Von Streber

C.P. Angelo Calderini
Director

Unidad Operativa de Contratación

Fausto Von Streber
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Dependencia y cargo que desempeña: *Director de Tecnologías de la Información y Comunicación*

- **Justificación técnica que respalda la objetividad, imparcialidad, regularidad y la razonabilidad o proporcionalidad de los requerimientos técnicos solicitados:**

Actualmente la institución cuenta con cuatro (4) equipos de firewall por hardware, los cuales han demostrado que ofrecen una protección avanzada contra una amplia gama de amenazas cibernéticas, incluidos virus, malware, ransomware y ataques de día cero, con los cuales han sido fundamentales para proteger nuestra red contra amenazas externas e internas.

Atendiendo la creciente complejidad y sofisticación de los ataques cibernéticos, consideramos necesario ampliar nuestra seguridad con dos (2) equipos de firewall por hardware y su respectivo software de administración que garanticen la seguridad de nuestra infraestructura informática y filtre el tráfico en una red.

Cabe destacar que los equipos de firewall por hardware proporcionan una protección adicional, ya que permiten una detención más precisa y, por ende, una respuesta más rápida a posibles amenazas, lo que incluido al software de administración de firewall permitirá gestionar y administrar de manera centralizada todas las políticas de seguridad, simplificando su configuración y supervisión.

La renovación de las 2 (dos) licencias administradoras de Email Protection y Web Server Protection de administración de los equipos de firewall Sophos XGS 6500 con que se cuenta simplificará la configuración, supervisión y gestión de la seguridad en toda la red, facilitando el trabajo del personal de la Dirección de TIC, garantizando una respuesta rápida a posibles amenazas y ayudará a la Institución a cumplir con las normativas y estándares de seguridad cibernética. Estos escudos adicionales ofrecen una protección extra, detectando amenazas con mayor precisión y velocidad, siendo crucial esta inversión en seguridad para mantenernos un paso adelante en la protección de nuestra infraestructura digital, previniendo así a la institución ser víctima del cibercrimen.

En resumen, la adquisición de equipos de firewall por hardware como las licencias de Email Protection y Web Server Protection tiene como objeto de fortalecer la seguridad de red interna como externa de la institución.

- **Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes.**

Atendiendo la particularidad detallada en las especificaciones técnicas, entre las cuales como principal característica se mencionan marca y modelo de los equipos existentes en la institución, es necesario indicar que los potenciales oferentes deben poseer ciertas condiciones para garantizar la calidad del bien, situación que no debería ser consideradas como limitaciones para la participación de éstos.

- **Si en las bases licitatorias se indica una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial.**

C.P. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Strober
Director de T.I.C.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
Y COMUNICACIÓN

Es importante indicar que en la elaboración de las especificaciones, resultó necesaria la mención de las marcas y modelos de los equipos existentes en la institución, aclarando que tienen un carácter meramente referencial, en ese sentido; para la provisión, se considera necesario que los potenciales oferentes posean un acabado conocimiento de lo pretendido, a los efectos de satisfacer íntegra, eficaz y efectivamente la necesidad institucional, conforme se detalla a continuación:

III) ESPECIFICACIONES TÉCNICAS

Teniendo en cuenta la necesidad institucional cuya satisfacción se pretende, esta Dirección ha diseñado las especificaciones técnicas con las características específicas de los bienes pretendidos, que constituyen las más adecuadas teniendo en cuenta el relevamiento de datos realizado, el cual ayudó a determinar todos los detalles y requisitos que debe cumplir los equipos de impresión.

Bienes Requeridos

Especificaciones Técnicas		
LOTE N° 1 - EQUIPO FIREWALL PARA SEGURIDAD PERIMETRAL Y SOFTWARE DE PROTECCIÓN PARA SERVIDOR WEB Y CORREO		
Ítem N° 1 - EQUIPO FIREWALL PARA SEGURIDAD PERIMETRAL		
Características	Descripción Técnica	Mínimo Requerido
Descripción General	Interfaz de usuario optimizada y especialmente diseñada para la administración de reglas de firewall para grandes conjuntos de reglas con agrupación con características de reglas de un vistazo e indicadores de aplicación.	Exigido
	Compatibilidad con autenticación de dos factores (contraseña de un solo uso) para acceso de administrador, portal de usuario, IPSec y SSL VPN.	Exigido
	Administración basada en roles.	Exigido
	Herramientas avanzadas de resolución de problemas en GUI (por ejemplo, captura de paquetes).	Exigido
	Interfaz de línea de comandos completa (CLI).	Exigido
	Soporte de alta disponibilidad (HA) para agrupar dos dispositivos en modo activo-activo o activo-pasivo con configuración de HA rápida plug-and-play según sea requerido.	Exigido
	Notificación automatizada de actualización de firmware con un sencillo proceso de actualización automatizado y funciones de reversión.	Exigido
	Definiciones de objetos de sistema reutilizables para redes, servicios, hosts, periodos de tiempo, usuarios y grupos, clientes y servidores.	Exigido
	Portal de usuario de autoservicio.	Exigido
	Seguimiento de cambios de configuración.	Exigido
	Control de acceso a dispositivos flexible para servicios por zonas.	Exigido
	Opciones de notificación de captura de correo electrónico o SNMP.	Exigido
	Compatibilidad con SNMPv3 y Netflow.	Exigido
	Soporte de administración central a través de la consola unificada basada en la nube o local	Exigido
	Notificaciones automáticas por correo electrónico para cualquier evento importante.	Exigido
	Configuraciones de copia de seguridad y restauración: localmente, a través de FTP o correo electrónico; bajo demanda, diariamente, semanalmente o mensualmente.	Exigido
	Monitoreo de flujo en tiempo real.	Exigido
	SNMP con una MIB personalizada y soporte para túneles VPN IPSec.	Exigido

C.P. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Strebe
Director de T.I.C.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Requerimientos Mínimos	Firewall Throughput: 115 Gbps mínimo medido en 64 byte UDP o medido usando tráfico HTTP y tamaño de respuesta de 512 KB.	Exigido
	Threat Protection Throughput: 17.5 Gbps mínimo usando tamaño de respuesta HTTP de 200 KB o Enterprise Mix.	Exigido
	IPsec VPN Throughput: 100 Gbps mínimo.	Exigido
	08 GbE Interfaces de cobre como mínimo.	Exigido
	12 SFP+ 10 GbE de fibra como mínimo.	Exigido
	Rendimiento IPS 45 Gbps mínimo.	Exigido
	Conexiones Simultaneas 39.000.000 mínimo.	Exigido
	Fuente de Poder redundante.	Exigido
Central Firewall Management	Debe contar con una consola web (https) basada en la nube o local.	Exigido
	La administración de directivas de grupo permite que los objetos, la configuración y las directivas se modifiquen una vez y se sincronicen automáticamente con todos los firewalls del grupo.	Exigido
	El Administrador de tareas proporciona una pista de auditoría histórica completa y supervisión del estado de los cambios en las directivas de grupo.	Exigido
	Programación de actualizaciones de firmware.	Exigido
	Informes de múltiples firewalls entre grupos de firewall.	Exigido
	Guardar, programar y exportar informes desde la consola.	Exigido
Firewall, Networking & Routing	Firewall de inspección profunda de paquetes.	Exigido
	Arquitectura de procesamiento de paquetes que proporciona altos niveles de visibilidad, protección y rendimiento a través del procesamiento detallado de paquetes.	Exigido
	Inspección TLS con alto rendimiento, soporte para TLS 1.3 o superior sin degradación, puertos independientes, políticas de nivel empresarial, visibilidad única del panel y solución de problemas de compatibilidad.	Exigido
	Motor DPI que proporciona protección de escaneo de flujos para IPS, AV, Web, App Control y TLS Inspección en un solo motor de alto rendimiento.	Exigido
	La solución debe proporcionar políticas basadas en usuarios, grupos, horarios o redes.	Exigido
	Políticas de tiempo de acceso por usuario/grupo.	Exigido
	Aplicar directivas en todas las zonas, redes o por tipo de servicio.	Exigido
	Firewall basado en zonas.	Exigido
	Soporte completo de VLAN.	Exigido
	Aislamiento de zonas y VLAN y compatibilidad con políticas basadas en zonas.	Exigido
	Zonas personalizadas en LAN o DMZ.	Exigido
	Políticas NAT personalizables con enmascaramiento de IP y soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un conveniente asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics.	Exigido
	Enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF) con soporte completo de VLAN 802.1Q.	Exigido
	Enrutamiento de multidifusión independiente del protocolo con snooping IGMP.	Exigido
	Puente con soporte STP y reenvío de difusión ARP.	Exigido
	Compatibilidad y etiquetado de VLAN DHCP.	Exigido
	Compatibilidad con puentes VLAN.	Exigido
	Soporte de Jumbo Frames.	Exigido
	Agregación de enlaces de interfaz 802.3ad.	Exigido
	Configuración completa de DNS, DHCP y NTP.	Exigido
	DNS dinámico (DDNS).	Exigido
SD-WAN	Certificación de aprobación del programa IPv6 Ready Logo.	Exigido
	Selección y enrutamiento de rutas de aplicaciones, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP.	Exigido
	Enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas.	Exigido
	Soporte VPN robusto que incluye IPsec y SSL VPN.	Exigido
	Orquestación VPN centralizada.	Exigido
	Integración con Azure Virtual WAN para una red de superposición SD-WAN completa.	Exigido

C.F. Angelo Calderini
Director

Unidad Operativa de Contratación

Avda. Eusebio Ayala 2759 e/Santa Cruz de la Sierra – Tel: (+59521) 6180361, Asunción – Paraguay

dramirez@tsje.gov.py/fausto@tsje.gov.py

Fausto Von Streber
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Base Traffic Shaping & Quotas	Configuración flexible del tráfico basado en la red o en el usuario (QoS) (opciones mejoradas de configuración del tráfico web y de aplicaciones incluido Web Protection).	Exigido
	Establecer cuotas de tráfico basadas en el usuario en la carga/descarga o tráfico total y cíclico o no cíclico.	Exigido
	Optimización de VoIP en tiempo real.	Exigido
Authentication	Autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS+.	Exigido
	Inicio de sesión único: Active Directory, eDirectory y RADIUS.	Exigido
	Compatibilidad con agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64.	Exigido
	Autenticación SSO del navegador: autenticación de proxy transparente (NTLM) y Kerberos.	Exigido
	Portal cautivo del navegador.	Exigido
	Servicios de autenticación para IPSec, SSL, L2TP, PPTP.	Exigido
	Integración de Azure AD.	Exigido
Base VPN	Compatibilidad con la creación de usuarios con formato UPN para la autenticación RADIUS.	Exigido
	Túneles VPN IPSec y SSL.	Exigido
	VPN de sitio a sitio: SSL, IPSec, AES/3DES de 256 bits, PFS, RSA, X.509 certificados, clave pre-compartida.	Exigido
	VPN basada en rutas.	Exigido
	Acceso remoto: SSL, IPsec, soporte de cliente VPN para iPhone / iPad / Cisco / Android.	Exigido
	Soporte IKEv2.	Exigido
	Cliente SSL para Windows y descarga de configuración a través del portal de usuario.	Exigido
	Aplicación de TLS 1.2 para túneles VPN SSL de sitio a sitio y de acceso remoto.	Exigido
Connect VPN Client y clientless	Compatibilidad con IPSec y SSL.	Exigido
	Fácil aprovisionamiento e implementación.	Exigido
	Licencias ilimitadas de acceso remoto SSL incluidas sin cargo adicional.	Exigido
	Autenticación: clave precompartida (PSK), PKI (X.509), token y XAUTH.	Exigido
	Túnel dividido inteligente para un enrutamiento óptimo del tráfico.	Exigido
	Compatibilidad con NAT-traversal.	Exigido
	Client-monitor para obtener una visión general gráfica del estado de la conexión.	Exigido
	Compatibilidad con Mac y Windows.	Exigido
Intrusion Prevention (IPS) y ATP	Portal de autoservicio HTML5 cifrado único con soporte para RDP, HTTP, HTTPS, SSH, Telnet y VNC.	Exigido
	Motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre la base de reglas de firewall para obtener el máximo rendimiento y protección.	Exigido
	Protección contra amenazas de día cero.	Exigido
	Defensas perimetrales.	Exigido
	Selección granular de categorías.	Exigido
	Compatibilidad con firmas IPS personalizadas.	Exigido
	Los filtros inteligentes de directiva IPS habilitan directivas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones.	Exigido
	Protección avanzada contra amenazas (detectar y bloquear el tráfico de red que intenta ponerse en contacto con servidores de comando y control mediante DNS, AFC y firewall de varias capas).	Exigido
Web Protection and Control	Proxy totalmente transparente para antimalware y filtrado web.	Exigido
	Protección avanzada contra amenazas mejorada.	Exigido
	Base de datos de filtro de URL con millones de sitios en 92 categorías.	Exigido
	Políticas de tiempo de cuota de navegación por usuario/grupo.	Exigido
	Políticas de tiempo de acceso por usuario/grupo.	Exigido
	Escaneo de malware: bloquee todas las formas de virus, malware web, troyanos y spyware en HTTP/S, FTP y correo electrónico basado en la web.	Exigido
	Protección avanzada contra malware web con emulación de JavaScript.	Exigido

Dr. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Streber
Director de T.I.C.

C.P. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Streben
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

	La interfaz de usuario intuitiva proporciona una representación gráfica de los datos.	Exigido
	El panel de informes proporciona una vista rápida de los eventos de las últimas 24 horas.	Exigido
	Debe identificar fácilmente las actividades de red, las tendencias y los posibles ataques.	Exigido
	Copia de seguridad sencilla de los registros con recuperación rápida para las necesidades de auditoría.	Exigido
	Posibilidad de crear informes personalizados con potentes herramientas de visualización.	Exigido
	Búsqueda y visualización de Syslog.	Exigido
	Almacenamiento de datos en Syslog.	Exigido
	Informes bajo demanda.	Exigido
	Almacenamiento en la OnePremise o nube de 7 días para informes de Central Firewall.	Exigido
	Informe sobre la nueva aplicación en la nube (CASB).	Exigido
	Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS.	Exigido
	Anonimización de informes.	Exigido
	Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.	Exigido
	Exportar informes como HTML, PDF, Excel (XLS).	Exigido
	Personalización de la retención de registros por categoría.	Exigido
Autorización	El oferente deberá ser representante o distribuidor autorizado de los bienes ofertados. Se deberá presentar una Autorización del Fabricante para presentar oferta y deberá estar dirigida a la licitación de referencia.	Exigido
Garantía de fábrica	Garantía de al menos 3 años de fábrica de los equipos ofertados a partir de la recepción por parte del TSJE. La carta de garantía deberá estar firmada por el fabricante o distribuidor autorizado en el Paraguay de la marca de los equipos ofertados. La garantía permite el reemplazo de partes sin costo para la convocante por problemas de fabricación o diseño de los equipos ofertados.	Exigido

Ítem N° 2 - PROTECCIÓN PARA SERVIDOR WEB Y CORREO		
Descripción Técnica		Mínimo Requerido
Protección de Servidor WEB		
Web Application Firewall Protection	Protección de servidores web mediante autenticación de proxy inverso.	Exigido
	Soporte para wildcard domains.	Exigido
	Protección de manipulación de formularios.	Exigido
	Protección contra ataques XSS.	Exigido
	Protección contra ataques DoS.	Exigido
	Protección de servidores web contra exploits.	Exigido
	Descarga de cifrado HTTPS (TLS/SSL).	Exigido
	Protección de cookies.	Exigido
	Reenvío de URL a servidores web específicos.	Exigido
	Posibilidad de vincular sesiones a un servidor web o reenvío de todas las solicitudes a un servidor web principal.	Exigido
	Omita las comprobaciones individuales de forma granular según sea necesario.	Exigido
	Permitir/Bloquear rangos de IP.	Exigido
	Compatibilidad con comodines para rutas de acceso y dominios de servidor.	Exigido
	Anexar automáticamente un prefijo/sufijo para la autenticación.	Exigido
Protección para servidor de Correo		
	Soporte de protección continua post entrega.	Exigido

C.P. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Streber
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Email Protection and Control	Análisis de correo electrónico con compatibilidad con SMTP, POP3 e IMAP.	Exigido
	Soporte de listas de control de Contenido.	Exigido
	Bloquear spam y malware durante la transacción SMTP.	Exigido
	Protección antispam DKIM y DMARK.	Exigido
	Lista gris de spam y protección del Marco de directivas de remitentes (SPF).	Exigido
	Verificación de destinatarios para direcciones de correo electrónico mal escritas.	Exigido
	Protección contra phishing y suplantación de identidad.	Exigido
	Búsquedas en la nube en tiempo real para obtener la inteligencia de amenazas más reciente.	Exigido
	Actualizaciones automáticas de firmas y patrones.	Exigido
	Compatibilidad con hosts inteligentes para relés salientes.	Exigido
	Detección/bloqueo/escaneo de archivos adjuntos.	Exigido
	Soporte de escaneo de malware y antispam.	Exigido
	Detecta urls de phishing dentro de los correos electrónicos.	Exigido
	Soporte de reglas de análisis de contenido predefinidos o creación de propias reglas personalizadas basadas en una variedad de criterios con opciones de política granulares y excepciones.	Exigido
	Soporte de cifrado TLS.	Exigido
	S/MIME.	Exigido
	Comprobación de dominios.	Exigido
	Protección contra reescritura de direcciones URL en el momento del clic.	Exigido
Email Quarantine Management	Opciones de resumen y notificaciones de cuarentena de spam.	Exigido
	Cuarentenas de malware y spam con opciones de búsqueda y filtro por fecha, remitente, destinatario, asunto y motivo con opción de liberar y eliminar mensajes.	Exigido
	Portal de usuario de autoservicio para ver y liberar mensajes en cuarentena.	Exigido
Email Encryption and DLP	Gestión de políticas DLP con múltiples Reglas.	Opcional
	Cifrado basado en imposición.	Opcional
	Cifrado basado en extracción.	Opcional
	Completamente transparente, no se requiere software o cliente adicional.	Opcional
	Motor DLP con escaneo automático de correos electrónicos y archivos adjuntos en busca de datos confidenciales.	Opcional
Validez de licencias	12 meses.	Exigido

LOTE 2 - ACTUALIZACIÓN DE LICENCIAS PARA PROTECCIÓN PARA SERVIDOR WEB Y CORREO PARA SOPHOS XGS 6500	
Ítem N° 1 - ACTUALIZACIÓN DE LICENCIAS PARA PROTECCIÓN PARA SERVIDOR WEB Y CORREO	Mínimo Requerido
Licencia para 1 (un) equipo. El Software deberá incluir las siguientes funcionalidades: 1) Protección de Servidor WEB. - Autenticación de proxy inverso. 2) Protección para servidor de Correo. - Protección y control del correo electrónico. - Gestión de cuarentena de correo electrónico. - Cifrado de correo electrónico y DLP. Validez de licencias: 12 meses.	Exigido

Por lo expuesto, la Dirección de Tecnologías de la Información y Comunicación considera que las Especificaciones Técnicas de los bienes solicitados se encuentran debidamente sustentadas técnicamente, conforme a la necesidad institucional, atendiendo a que las mismas

C.P. Angelo Calderini
Director
Unidad Operativa de Contratación

Fausto Von Strebe
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

fueron diseñadas a los efectos de asegurar las mejores condiciones de contratación en cuanto a oportunidad, calidad y costo se refiere.

C. P. Ángel...
Director de TIC
Es mi dictamen.-
Unidad Operativa de Contratación



Lic. Fausto Von Streber
Director de TIC

