



### FICHA TÉCNICA

Servicio:	Servicio de actualización integral de la infraestructura tecnológica para el sitio alternativo del Instituto Registral y Catastral del Estado de Nuevo León (IRCNL).	Cantidad:	0 1
-----------	--	-----------	--------

Componente	Características
Servicio solicitado (Partida única)	<p><b>Justificación del servicio:</b></p> <p>El Instituto Registral y Catastral del Estado de Nuevo León (IRCNL) requiere fortalecer su infraestructura tecnológica mediante la implementación de un sitio alternativo que garantice la continuidad operativa y la disponibilidad de los servicios institucionales. Actualmente, los sistemas críticos del IRCNL se alojan en una infraestructura central que no cuenta con un entorno replicado ni con una solución integral de recuperación ante desastres (DRP), lo que representa un riesgo operativo y de seguridad de la información.</p> <p>La obsolescencia de los equipos actuales representa otro riesgo latente de fallas, pérdida de datos y vulnerabilidades de seguridad, afectando directamente la atención a la ciudadanía y la integridad de los sistemas institucionales. Este proyecto busca asegurar una infraestructura moderna, resiliente y preparada para enfrentar los desafíos tecnológicos actuales y futuros.</p> <p><b>Alcance del servicio:</b></p> <p><b>Suministro de equipo, instalación física, configuración lógica y puesta en operación funcional</b> de una infraestructura tecnológica integral para el sitio alternativo compuesta por servidores físicos de alto rendimiento con procesadores de gama alta, RAM expandible y conectividad GbE; Arreglo de almacenamiento unificado tipo SAN con replicación bidireccional y protocolos avanzados de encriptación para servidores virtualizados; Solución integral de respaldo centralizado con inmutabilidad de información, compatibilidad con múltiples sistemas operativos y bases de datos y replicación WAN para todos los servidores virtualizados; Solución integral de conmutadores de red de alta velocidad; Solución para recuperación ante desastres (DRP); Licenciamiento y todo lo requerido para la instalación de la infraestructura tecnológica integral propuesta. Además, soporte 24x7, un recurso humano dedicado en sitio durante 29 meses, capacitación y transferencia</p>



de conocimiento para el Instituto Registral y Catastral del Estado de Nuevo León (IRCNL) con los siguientes **componentes** y **especificaciones técnicas mínimas aceptables**:

1. Componente **servidores físicos**: Cuatro (4) servidores físicos independientes para operar máquinas virtuales.
2. Componente **gabinetes** (racks cerrados): Dos (2) gabinetes.
3. Componente **unidades de distribución de energía** (PDU): Cuatro (4) unidades de distribución de energía, con al menos dos (2) para cada gabinete.
4. Componente **almacenamiento unificado**: Un (1) arreglo de almacenamiento tipo SAN por canal de fibra para máquinas virtuales.
5. Componente **respaldo centralizado**: Una (1) solución de respaldo para máquinas virtuales.
6. Componente **conmutadores de red** (switches):
  - 6.1. Dos (2) switches LAN para almacenamiento tipo SAN.
  - 6.2. Dos (4) switches LAN de transporte.
  - 6.3. Un (1) switch LAN para administración.
7. Componente **solución de recuperación ante desastres (DRP)**: Una (1) solución de continuidad de negocio y recuperación ante desastres (DRP) para entornos virtualizados con integración nativa.
8. Componente **licenciamiento, garantías y soporte**.
9. Componente **recurso humano dedicado**: Un (1) recurso humano en sitio.
10. Componente **capacitación y transferencia de conocimiento**.
11. **Criterios de homologación tecnológica**.

**Especificaciones técnicas:**

A continuación, las características técnicas mínimas aceptables por componente:

1. Componente **servidores físicos**:
  - 1.1. Grupo de servidores con capacidad total para almacenar hasta 80 máquinas virtuales con software de virtualización y administración con al menos 954 vCPUs.
  - 1.2. Cada servidor físico, con dos (2) procesadores Intel Xeon a 2.8 GHz con al menos 32 núcleos cada procesador.
  - 1.3. Cada servidor físico, con al menos mil veinticuatro (1024) Gigabytes en RAM (1TB) con capacidad de crecimiento al doble solo añadiendo más DIMMs, es decir sin necesidad de cambiar o eliminar DIMMs, del tipo DDR5-5200.



	<p>1.4. Cada servidor físico, con dos (2) discos de arranque (boot) de 480GB, tipo estado sólido (SSD), interfaz SATA, en arreglo tipo RAID 1.</p> <p>1.5. Cada servidor físico, con al menos dos (2) puertos de red de alta velocidad a 25 GbE con interfaces SFP28 en al menos dos (2) tarjetas.</p> <p>1.6. Cada servidor físico, con al menor dos (2) tarjetas con dos (2) puertos fibra canal de alta velocidad FC de 32Gb cada una para conexión a almacenamiento tipo SAN.</p> <p>1.7. Cada servidor físico, con al menos un módulo de administración fuera de banda con capacidades remotas.</p> <p>1.8. Cada servidor físico, con un módulo de plataforma de confianza (TPM, por sus siglas en inglés: Trusted Platform Module) versión 2.0 V5, para almacenar y gestionar de manera segura claves de cifrado, certificados y contraseñas.</p> <p>1.9. Cada servidor físico con al menos dos (2) fuentes de alimentación para redundancia.</p> <p>1.10. Cada servidor físico, de dos (2) unidades de rack y con rieles para montaje en rack.</p> <p>1.11. Cada servidor físico con al menos seis (6) slots PCI y al menos uno (1) de ellos Gen5 x16 de tipo Full Length.</p> <p>1.12. Cada servidor físico debe soportar hasta dos (2) tarjetas de unidad de procesamiento gráfico (GPU, por sus siglas en inglés: Graphics Processing Unit) de doble ancho de hasta 350 Watts.</p> <p>2. Componente <b>gabinetes</b> (racks cerrados):</p> <p>Diseñados para albergar grupos de servidores y dispositivos de red dentro de un entorno de centro de datos o sala de servidores.</p> <p>2.1. Tamaño estándar de 19 pulgadas.</p> <p>2.2. Altura de 42 unidades (U).</p> <p>2.3. Ancho de 750 mm.</p> <p>2.4. Profundidad de 1200 mm.</p> <p>2.5. Color negro, adecuado para la estética y entorno profesional de los centros de datos.</p> <p>2.6. Kit de ruedas para facilitar el desplazamiento.</p> <p>2.7. Pie nivelador del gabinete para asegurar la estabilidad.</p> <p>2.8. Puerta trasera perforada para ventilación adecuada y acceso al equipo.</p> <p>2.9. Paneles laterales para protección y seguridad de la infraestructura.</p> <p>2.10. Puerta frontal que proporcione acceso seguro y controlado.</p>
--	---



	<p>2.11. Carriles de montaje verticales ajustables para adaptarse a diferentes equipos.</p> <p>2.12. Techo de protección.</p> <p>2.13. Llaves para asegurar el acceso restringido a la infraestructura.</p> <p>2.14. Puerta trasera perforada dividida para una mejor ventilación.</p> <p>2.15. Soportes del gabinete para estabilizar equipos por dentro.</p> <p>2.16. Montaje incluyendo todos los componentes necesarios para su instalación.</p> <p>2.17. Placas y tornillos necesarios para el montaje de la infraestructura.</p> <p>2.18. Paneles ciegos para cubrir espacios no utilizados y mejorar la circulación de aire.</p> <p>2.19. Organizador de cables para gestionar el cableado y mantener un entorno ordenado.</p> <p>2.20. Organizador horizontal en base a la infraestructura propuesta para facilitar la gestión del cableado y componentes.</p> <p>3. Componente <b>unidades de distribución de energía</b> (PDU):</p> <p>3.1. PDU del tipo medición, con monitor de carga en tiempo real y alarmas configurables.</p> <p>3.2. Conector/enchufe NEMA L6-30P.</p> <p>3.3. Receptáculo IEC 60320 C13 y IEC 603020 C19.</p> <p>3.4. Detalle del receptáculo 36 x IEC 60320 C13 y 6 x IEC 60320 C19.</p> <p>3.5. Tipo de protección con sobrecargas.</p> <p>3.6. Voltaje de entrada: 200V a 208V.</p> <p>3.7. Voltaje de salida: 200 VAC a 208 VAC.</p> <p>3.8. Protocolos de gestión: SNMP y Telnet.</p> <p>3.9. Tipo de montaje en gabinete (rack cerrado).</p> <p>3.10. Altura del rack 0U.</p> <p>3.11. Longitud de cable de 3 m.</p> <p>3.12. Altura 1791 mm.</p> <p>3.13. Anchura 56 mm.</p> <p>3.14. Profundidad 44 mm.</p> <p>3.15. Peso (aproximado) 6.84 kg.</p> <p>3.16. Orientación de montaje vertical.</p> <p>3.17. Ubicación de lado.</p> <p>3.18. Con gestión remota e interfaces Web, SNMP, Telnet, compatible con EcoStruxure IT.</p> <p>3.19. Deben admitir al menos 4 PDUs en cascada con una sola IP</p> <p>4. Componente <b>almacenamiento unificado</b>:</p>
--	--



	<ol style="list-style-type: none"> <li>4.1. Capacidad del almacenamiento unificado para máquinas virtuales de al menos 50 TB usables con un factor de compresión garantizado de 3:1 para contar con al menos 150 TB de capacidad usables.</li> <li>4.2. Contar con memoria cache de al menos 768 GB tipo DRAM (contar con al menos 384 GB por controladora).</li> <li>4.3. Cada controladora deberá tener al menos 2 procesadores Intel Xeon.</li> <li>4.4. Debe soportar un crecimiento de al menos 6 controladoras adicionales.</li> <li>4.5. Redundancia en componentes como: Controladoras, discos, fuentes de alimentación, ventiladores, baterías, sin presentar punto único de falla.</li> <li>4.6. Capacidad de enviar información contenida en la memoria cache a disco o memoria no volátil en caso de falla eléctrica.</li> <li>4.7. Soportar la configuración de controladoras o nodos de diferentes capacidades de procesamiento y memoria cache en el mismo sistema sin afectar el desempeño y de manera no disruptiva.</li> <li>4.8. Módulo de doble controladora redundante para brindar protocolos de bloque (SAN) y archivo (NAS) de manera activa / activa.</li> <li>4.9. Soportar el cifrado FIPS 140-2 en los discos de datos.</li> <li>4.10. Soportar conexiones a 100 GbE iSCSI.</li> <li>4.11. Con al menos ocho (8) puertos FC de 32Gb.</li> <li>4.12. Con al menos ocho (8) Puertos para conexión de red 25GbE.</li> <li>4.13. Con al menos dos (2) discos NVRAM que soporte cache de lectura y escritura en Raid 1 o Mirror.</li> <li>4.14. Soportar al menos los siguientes tipos de discos: NVMe SSD.</li> <li>4.15. Soportar al menos una disponibilidad 99.9999 %.</li> <li>4.16. Soportar los siguientes protocolos: File, Block, vVols (VVMs) 2.0; NFS (v3, v4, 4.1); CIFS (SMB 1, 2, 3, 3.02 y 3.1.1); FTP y SFTP; FC, iSCSI, NVMe/FC, NVMe/TCP.</li> <li>4.17. Soportar también estos otros protocolos y servicios: LDAP; NTLM; SMTP, NTP; RSVD v1; ARP; ICMP; NIS; NSM; DFS; ABE for SMB; NDMP v1-v4; DAC; SNMP, VAAI y VASA.</li> <li>4.18. Soportar NVMe QLC SSD o NVMe TLC SSD.</li> <li>4.19. Sistema de configuración para soporte de al menos paridad simple o doble.</li> <li>4.20. Con replicación nativa, con la capacidad de ser bidireccional y síncrona, asíncrona y metro, sin necesidad de licenciamiento adicional y por medio de puertos de 10GbE o superior.</li> <li>4.21. Soportar <i>snapshots</i> inmutables.</li> </ol>
--	---



	<p>4.22. Componentes de File-sharing (CIFS y NFS) en el mismo gabinete.</p> <p>4.23. Proveer volúmenes a servidores: HP-UX, IBM AIX, RHEL, SUSE SLES, Oracle Solaris, Windows 2016 o superior, hipervisor VMWare ESX versión 7.0 o superior.</p> <p>4.24. Sistema de administración y monitoreo local y remota, gráfico y por línea de comando, para todos los componentes del sistema.</p> <p>4.25. Dispositivo de almacenamiento con arquitectura modular a nivel SAN / NAS, para bloques, archivos y vVols en un solo sistema y con una sola consola de administración.</p> <p>4.26. No Gateway externo.</p> <p>4.27. Sistema operativo desarrollado propietario de la misma marca del fabricante del hardware con capacidad para entregar de modo directo los servicios de SAN/NAS.</p> <p>4.28. El sistema operativo del sistema de almacenamiento debe estar basado en contenedores.</p> <p>5. Componente <b>respaldo centralizado</b>:</p> <p>5.1. Almacenamiento orientado a respaldo con de duplicación en línea.</p> <p>5.2. Replicación de datos entre equipos de almacenamiento de respaldo a través de WAN, siendo bidireccional y replicando datos de duplicados para reducir el ancho de banda requerido.</p> <p>5.3. Administrar de forma centralizada las estrategias de respaldo, recuperación y migración de información entre servidores.</p> <p>5.4. Con una capacidad de almacenamiento equipado de al menos 150 TB usables.</p> <p>5.5. Compatibilidad multiprotocolo: NFS, CIFS, DD Boost, VTL, NDMP.</p> <p>5.6. Protección de datos: <i>Snapshots</i>, replicación, cifrado en reposo y en tránsito.</p> <p>5.7. Integración nativa con software de respaldo de terceros.</p> <p>5.8. Soporte para replicación hacia nube pública (AWS, Azure, <b>Google Cloud</b>, <b>Alibaba Cloud</b>) mediante Cloud Tier.</p> <p>5.9. Sistemas de archivos cifrados (FIPS 140-2) y arranque seguro.</p> <p>5.10. Certificaciones: FIPS 140-2.</p> <p>5.11. Cifrado de datos con al menos 256 bits (en tránsito y en reposo) de AES (Advanced Encryption Standard).</p> <p>5.12. Permitir la exclusión de archivos o carpetas dentro de la política de respaldo mediante filtros configurables.</p>
--	---



	<p>5.13. Debe soportar la recuperación a un punto específico en el tiempo y permitir la migración de datos entre servidores</p> <p>5.14. Autenticación basadas en roles (RBAC).</p> <p>5.15. Soporte para auditoría, syslog, alertas SNMP y STIGs.</p> <p>5.16. Soporte para VMware, Oracle RMAN, SAP HANA, Microsoft SQL, entre otros.</p> <p>5.17. La solución de respaldo centralizado deberá ser compatible con los siguientes sistemas operativos, bases de datos e hipervisores, así como con sus versiones futuras:</p> <p>5.17.1. IBM AIX: v7.1, 7.2 &amp; 7.3 TL2 SP2.</p> <p>5.17.2. Oracle Solaris: 10, 11.2, 11.13, 11.4.</p> <p>5.17.3. Microsoft SQL Server: 2014, 2016, 2017, 2019, 2022 CU8.</p> <p>5.17.4. Red Hat Enterprise Linux: v8.0 – 9.4.</p> <p>5.17.5. Suse Linux: 12, 15 SP4.</p> <p>5.17.6. Rocky Linux: 8.x, 9.x.</p> <p>5.17.7. Microsoft Windows Server: 2016, 2019, 2022.</p> <p>5.17.8. Microsoft Windows 10, 11.</p> <p>5.17.9. Ubuntu: 16.4, 18.04, 20.04.</p> <p>5.17.10. Debian: 11.x 12.x.</p> <p>5.17.11. Alma Linux: 8.x, 9.x.</p> <p>5.17.12. ESXi: 6.7, 7.0, 8.0, 8.0U1.</p> <p>5.17.13. SAP HANA: 1.x y 2.x en combinación con RHEL y SLES.</p> <p>5.18. Requerimientos de Hardware de Almacenamiento:</p> <p>5.18.1. Un (1) puerto Ethernet para administración.</p> <p>5.18.2. Cuatro (4) puertos 25GbE ópticos SFP28.</p> <p>5.18.3. Capacidad de transferencia de al menos 33 TB/hora.</p> <p>5.18.4. Soporte para conexiones FC y 25GbE, hasta 16 puertos Ethernet 10Gb BaseT, 12 puertos FC 16/32 Gb, 16 puertos Ethernet 10Gb SFP+, 6 puertos Ethernet 25Gb SFP+.</p> <p>5.18.5. Capacidad de 150 TB usables.</p> <p>5.18.6. Incluir características de de duplicación.</p> <p>5.18.7. Incluir los periodos de retención indicados en este documento.</p> <p>5.18.8. Soportar firmware firmado criptográficamente, Secure Boot, Secure Erase, Silicon Root of Trust, System Lockdown</p> <p>5.18.9. El sistema operativo del sistema de almacenamiento debe estar basado en contenedores.</p> <p>5.19. Generar al menos los siguientes tipos de reportes:</p> <p>5.19.1. Cantidad de información transferida durante un periodo de tiempo.</p> <p>5.19.2. Resumen del estado actual de las tareas de respaldo.</p> <p>5.19.3. Reporte de servidores protegidos.</p>
--	---



	<p>5.20. Soportar licenciamiento para respaldar servidores con los siguientes sistemas operativos: Windows, IBM, AIX y Linux, así como las versiones más recientes de dichos sistemas operativos durante la vigencia del contrato.</p> <p>5.21. Que permita recuperar la información de al menos de 30 días atrás.</p> <p>5.22. Tener la funcionalidad o mecanismo de bloqueo de retención.</p> <p>5.23. Que permita establecer políticas de retención en las divisiones lógicas del sistema.</p> <p>5.24. Que impida la eliminación o modificación de archivos durante un periodo de tiempo predefinido, incluso por usuario con privilegios de administrador.</p> <p>5.25. Que permita configurar periodos de retención mínimos de 12 horas y hasta de 70 años; en intervalos de tiempo que pueden ser de minutos, horas, días, meses o años.</p> <p>5.26. Tener una capacidad de recuperación de un ciclo de 4 semanas y un respaldo mensual para proteger los datos, con la estimación realizada se pueden recuperar hasta 30 días, aproximadamente y con la funcionalidad o el mecanismo de bloqueo de retención activo puede ser inmutable.</p> <p>Para garantizar la protección inalterable de la información respaldada, la funcionalidad o mecanismo de bloqueo de retención, permite establecer políticas de retención en los MTree (divisiones lógicas del sistema). Esta funcionalidad impide la eliminación o modificación de archivos durante un periodo predefinido, incluso por usuarios con privilegios administrativos.</p> <p>Parámetros de configuración:</p> <ul style="list-style-type: none"> <li>• Período mínimo de retención permitido: 12 horas</li> <li>• Período máximo de retención permitido: 70 años</li> <li>• El período mínimo debe ser menor al período máximo configurado</li> </ul> <p>Unidades permitidas para los períodos de retención: Minutos, horas, días, meses y años.</p> <p>6. Componente <b>conmutadores de red</b> (switches):</p> <p>6.1. <u>Dos (2) switches LAN para almacenamiento tipo SAN.</u></p> <p>6.1.1. Cada switch, con al menos ocho (8) transceptor tipo SFP de 32 Gb/s, optimizados para conexiones de alto rendimiento FC de 32 Gb/s.</p>
--	---





	<p>6.1.2. Cada switch, con módulos SFP para crecimiento de hasta veinticuatro (24) puertos para soportar velocidades FC de 8/16/32/64 Gb/s.</p> <p>6.1.3. Cada switch, con fuente de poder y ventilador integrados.</p> <p>6.1.4. Con rendimiento de ancho de banda total mínimo de 3 Tb/s.</p> <p>6.1.5. Con capacidad de extensión de fábrica para conexión de FC e ISL Trunking.</p> <p>6.2. <u>Cuatro (4) switches LAN de transporte.</u></p> <p>6.2.1. Cada switch, con al menos veinticuatro (24) transceptor tipo SFP28 de 25 GbE.</p> <p>6.2.2. Con capacidad para crecer hasta cuarenta y ocho (48) transceptor tipo SFP28 de 25 GbE.</p> <p>6.2.3. Cada switch, con al menos cuatro (4) puertos de 100 GbE tipo QSFP28 para enlaces ascendentes (uplinks).</p> <p>6.2.4. Con capacidad de conmutación de al menos dos (2) Tbps (terabit por segundo) en modo duplex completo (full duplex).</p> <p>6.2.5. Cada switch, con capacidad de direcciones MAC de al menos 16,000 entradas.</p> <p>6.2.6. Cada switch con soporte de rutas IPv4 de hasta 128,000.</p> <p>6.2.7. Cada switch, con memoria de búfer de paquetes de 32 MB.</p> <p>6.2.8. Cada switch, con memoria del procesador (CPU) de 16 GB.</p> <p>6.2.9. Con funcionalidad de red multicapa (L2/L3) con soporte completo para IPv4, IPv6, OSPF, BGP, MLAG, VXLAN Gateway, QoS, ACL.</p> <p>6.2.10. Con fuentes de poder redundantes y de intercambio en caliente (hot swappable).</p> <p>6.2.11. Un (1) puerto de administración RJ45 dedicado para administración fuera de banda.</p> <p>6.3. <u>Un (1) switch LAN para administración:</u></p> <p>6.3.1. Con hasta cuarenta y ocho (48) puertos de acceso RJ45 de 1 GbE.</p> <p>6.3.2. Con hasta cuatro (4) puertos de alta velocidad SFP+ 10 GbE integrados.</p> <p>6.3.3. Con soporte para al menos dos (2) puertos QSFP28 de 100 GbE.</p> <p>6.3.4. Con capacidad de conmutación de al menos 576 Gb/s en modo duplex completo (full duplex).</p> <p>6.3.5. Con capacidad de reenvío de al menos 800 Mbps.</p> <p>6.3.6. Con funcionalidad de red multicapa (L2/L3) con soporte completo para IPv4, IPv6, OSPF, BGP, VRF, MLAG, VXLAN.</p>
--	--



	<p>6.3.7. Un (1) puerto de administración RJ45 dedicado para administración fuera de banda.</p> <p>6.3.8. Con fuentes de poder redundantes y de intercambio en caliente (hot swappable).</p> <p>7. Componente <b>solución de recuperación ante desastres (DRP)</b>:</p> <p>7.1. La solución debe garantizar respaldo, recuperación, detección de amenazas, orquestación de DRP y monitoreo integral para entornos virtuales, físicos y en la nube, con inmutabilidad, cifrado avanzado e integración con herramientas de seguridad y TI corporativas.</p> <p>Respaldo de entornos virtuales (VMware y Hyper-V)</p> <p>7.2. Soporte de copias de seguridad basadas en <i>snapshots</i> SAN.</p> <p>7.3. Respaldo incremental eficiente sin agentes, con detección automática de <i>snapshots</i> huérfanos y recursos insuficientes.</p> <p>7.4. Exclusión selectiva de discos, archivos temporales y bloques eliminados para optimizar rendimiento y espacio.</p> <p>7.5. Recuperación granular de aplicaciones (SQL, Exchange, Oracle, PostgreSQL) sin agentes adicionales.</p> <p>Protección de Datos Continua (CDP)</p> <p>7.6. Replicación asíncrona sin <i>snapshots</i> para minimizar RTO/RPO en VMware.</p> <p>7.7. Captura de todas las E/S de disco sin dependencia de hardware.</p> <p>7.8. Incluye failover planificado, failback, recuperación a nivel archivo y recuperación de elementos de aplicación.</p> <p>7.9. Visualizador de anomalías de I/O para rollback en caso de ransomware.</p> <p>Respaldo de entornos físicos</p> <p>7.10. Copia de seguridad de sistemas Windows, Linux, AIX, Solaris, Mac.</p> <p>7.11. Copias a nivel imagen/archivo con <i>Changed Block Tracking</i> (CBT).</p> <p>7.12. Plugins específicos para SQL, Oracle RMAN, SAP HANA y DB2; soporte SAP HANA en IBM Power.</p> <p>Recuperación integral y granular</p>
--	--



	<p>7.13. Portabilidad de respaldos sin infraestructura propietaria.</p> <p>7.14. <i>Instant Recovery</i> para VM y servidores físicos (Bare Metal Recovery).</p> <p>7.15. Soporte para recuperación en nube (AWS, Azure, Google Cloud).</p> <p>7.16. Verificación anti-malware antes de restaurar.</p> <p style="padding-left: 40px;">Recuperación de archivos y elementos de aplicación</p> <p>7.17. Restauración sin agentes en VMs físicas/virtuales.</p> <p>7.18. Exploradores para Active Directory, Exchange, SQL, Oracle, SAP HANA, MongoDB, PostgreSQL.</p> <p>7.19. Recuperación granular de bases de datos desde imágenes o RMAN.</p> <p style="padding-left: 40px;">Seguridad avanzada y detección de amenazas</p> <p>7.20. Escaneo in-line y off-line de backups con entropía, YARA y antivirus.</p> <p>7.21. Integración con SIEM, EDR/XDR, ServiceNow, generación de eventos SYSLOG.</p> <p>7.22. Autorización reforzada para eliminación de backups y credenciales de un solo uso.</p> <p style="padding-left: 40px;">Soporte multicanal de repositorios</p> <p>7.23. Repositorios en disco, cinta y nube (S3, Glacier, Azure Blob, Google Cloud) con inmutabilidad y de duplicación integrada.</p> <p>7.24. Integración con Data Domain, StoreOnce, ExaGrid, Infinidat.</p> <p>7.25. Copia a cinta con soporte WORM y visualización de contenido.</p> <p style="padding-left: 40px;">Monitoreo y reportería</p> <p>7.26. Dashboards de seguridad y compliance.</p> <p>7.27. Alertas proactivas de fallas, capacidad y cumplimiento de RPO.</p> <p>7.28. Generación de reportes de auditoría y planificación de capacidad.</p> <p>7.29. Integración bidireccional con ServiceNow.</p> <p style="padding-left: 40px;">Orquestación de recuperación</p> <p>7.30. Planes de DR automatizados para VMware y Hyper-V.</p> <p>7.31. Pruebas sin interrupción, medición de RTO/RPO y reportería compliance.</p> <p>7.32. Soporte de orquestación Cloud DR hacia Azure.</p>
--	--



	<p>7.33. Laboratorios de pruebas (Data Labs) y verificación de puntos de recuperación limpios</p> <p>Integración y automatización</p> <p>7.34. Consola con asistente GPT, analítica de seguridad.</p> <p>7.35. PowerShell SDK y REST API para integración con plataformas de terceros.</p> <p>7.36. Respaldo de máquinas virtuales en un repositorio inmutable.</p> <p>7.37. Permita la ejecución de pruebas de recuperación sin interrupción del entorno productivo.</p> <p>7.38. Genere informes detallados de todas las tareas de protección y recuperación.</p> <p>7.39. Garantice alta disponibilidad y continuidad operacional con tiempos mínimos o nulos de interrupción del servicio (tiempo de inactividad).</p> <p>Gestión y automatización:</p> <p>7.40. Plataforma basada en políticas de recuperación, permitiendo la automatización del proceso de protección y restauración de múltiples máquinas virtuales mediante planes de recuperación centralizados.</p> <p>7.41. Capacidad de orquestación avanzada, incluyendo flujos de trabajo automatizados y pruebas de recuperación en entornos aislados.</p> <p>Compatibilidad y despliegue:</p> <p>7.42. Compatible con cualquier sistema de almacenamiento, soportando replicación a nivel de hipervisor y con dispositivos de almacenamiento validados.</p> <p>7.43. Implementación 100 % en software, distribuido como dispositivo virtual (OVA - Aplicación Virtual Abierta), sin requerimiento de hardware dedicado.</p> <p>7.44. Consola de administración unificada con licenciamiento centralizado por suscripción.</p> <p>Replicación de datos:</p> <p>7.45. Soporte para replicación avanzada con Punto Objetivo de Recuperación (POR o RPO, por sus siglas en inglés) configurable hasta 1 minuto.</p> <p>7.46. Soporta replicación entre múltiples sitios geográficos o entre clústeres dentro del mismo centro de datos (CPD).</p> <p>7.47. Funciona como alternativa a las soluciones de replicación basadas en almacenamiento.</p>
--	--



Capacidades funcionales:

- 7.48. Orquestación de recuperación automatizada: Incluye ejecución automática de tareas de recuperación según orden definido, sin afectar la operación del entorno activo.
- 7.49. Pruebas de recuperación no disruptivas: Verificación de planes de recuperación en entornos de prueba sin afectar el entorno de producción.
- 7.50. Integración nativa con *Replication* y soporte de matrices de compatibilidad.
- 7.51. Recuperación priorizada de cargas de trabajo virtuales por grupos de máquinas virtuales.
- 7.52. Informes automáticos de ejecución con métricas detalladas de Tiempo Objetivo de Recuperación (TOR o RTO) y Punto Objetivo de Recuperación (RPO).
- 7.53. Personalización avanzada de red, con asignación de direcciones IP, ejecución de scripts personalizados y reconfiguración automática durante el proceso de recuperación.
- 7.54. Soporte para pruebas en caliente (hot testing), sin necesidad de suspensión de servicios.

Escenarios de uso:

- 7.55. Recuperación ante desastre total o parcial.
- 7.56. Migraciones planificadas de centros de datos o cargas específicas.
- 7.57. Operaciones de mantenimiento con mínima interrupción del servicio.
- 7.58. Balanceo de carga entre sitios para distribuir demanda operativa.

Topologías soportadas:

- 7.59. Activo/Activo Bidireccional: Ambos sitios operan de forma activa y pueden asumir la recuperación del otro en caso de contingencia.
- 7.60. Migración Planificada: Permite el traslado ordenado de servicios sin pérdida de datos.
- 7.61. Recuperación ante Desastre: Proceso automatizado para escenarios donde el sitio principal queda completamente fuera de servicio.

Proceso de recuperación automatizado:



	<p>7.62. Apagado ordenado de las máquinas virtuales en el sitio protegido.</p> <p>7.63. Sincronización de datos con el sitio de respaldo.</p> <p>7.64. Encendido secuencial de máquinas virtuales en el sitio de recuperación según el orden definido.</p> <p>7.65. Aplicación de configuraciones de red personalizadas y ejecución de scripts de inicialización o remediación.</p> <p>7.66. Generación de reportes automáticos post-recuperación.</p> <p>8. Componente <b>licenciamiento, garantías y soporte:</b></p> <p>8.1. Licenciamiento VMware para la plataforma de virtualización.</p> <p>8.2. Para el componente de servidores físicos, tres (3) años de soporte con atención en sitio, y la disponibilidad de que un administrador de cuenta de servicio asignado.</p> <p>8.3. Solución de orquestación de recuperación ante desastres compatible con la solución de virtualización utilizada actualmente para garantizar la alta disponibilidad y la continuidad tecnológica en virtualización integrando capacidades de replicación avanzada como <i>Replicator</i>, debe permitir la replicación de máquinas virtuales y ofrecer capacidades de recuperación de datos a nivel de máquina virtual, asegurando un tiempo mínimo de inactividad y una recuperación eficiente en caso de fallo.</p> <p>8.4. Para el componente <b>respaldo centralizado</b>, deberá soportar licenciamiento para respaldar servidores con los siguientes sistemas operativos: Windows, IBM, AIX y Linux, así como las versiones más recientes de dichos sistemas operativos durante la vigencia del contrato.</p> <p>9. Componente <b>recurso humano dedicado:</b></p> <p>9.1. Se deberá incluir un recurso humano en sitio, disponible durante el horario de oficina, con experiencia comprobada en plataformas de virtualización y entornos Windows.</p> <p>9.2. El profesional asignado debe contar con un mínimo de tres (3) años de experiencia en la gestión de plataformas de virtualización y sistemas operativos Windows, garantizando una administración adecuada y eficiente de las infraestructuras relacionadas.</p> <p>9.3. El recurso deberá estar dedicado al proyecto del IRCNL durante un periodo de <b>29 meses</b>, asegurando el cumplimiento de los plazos y la correcta ejecución de las tareas asignadas.</p>
--	---



	<p>10. Componente capacitación y transferencia de conocimiento.</p> <p>10.1. El proveedor deberá <b>capacitar</b> al recurso humano del IRCNL para operar la solución propuesta y brindar soporte técnico en caso de alguna falla relacionada con la infraestructura instalada cubriendo al menos los siguientes temas:</p> <p>10.1.1. <b>Virtualización:</b> Uso, administración y buenas prácticas de VMware o Hyper-V.</p> <p>10.1.2. <b>Almacenamiento:</b> Gestión de volúmenes, rendimiento, <i>snapshots</i> y replicación.</p> <p>10.1.3. <b>Respaldos (BaaS):</b> Configuración de jobs, restauraciones, inmutabilidad y retención.</p> <p>10.1.4. <b>Recuperación ante desastres (DRP):</b> Activación en la nube, pruebas de failover, RPO/RTO y failback.</p> <p>10.1.5. <b>Monitoreo:</b> Configuración y uso de plataformas de alertas y reportes.</p> <p>10.1.6. <b>Prácticas y simulacros:</b> Laboratorios, pruebas controladas y validación operativa.</p> <p>10.2. El proveedor deberá transferir el siguiente conocimiento:</p> <p>10.2.1. Documentación técnica: Manuales, diagramas, planes operativos y protocolos de emergencia.</p> <p>10.2.2. Cierre técnico y soporte inicial: Sesiones finales de transición y soporte post-implementación.</p> <p>11. Criterios de homologación tecnológica: Para garantizar la compatibilidad entre la solución de virtualización utilizada actualmente y la solución propuesta debe cumplir con las siguientes características mínimas aceptables:</p> <p><b>Plataforma de virtualización:</b></p> <p>11.1. Licenciamiento <b>VMware</b>.</p> <p>11.2. Hipervisor de tipo 1 (<i>bare-metal</i>), instalado directamente sobre el hardware físico, sin requerimiento de un sistema operativo intermedio.</p> <p>11.3. Capacidad de consolidación de cargas de trabajo mediante la virtualización de múltiples servidores físicos en máquinas virtuales independientes.</p> <p>11.4. Consola de administración basada en entorno web HTML5, con interfaz gráfica intuitiva y accesible desde navegadores compatibles.</p> <p>11.5. Soporte para funciones de gestión centralizada, alta disponibilidad (AD), y migración en caliente de máquinas virtuales (sin interrupción del servicio).</p>
--	--



	<p><b>Administración centralizada:</b></p> <p>11.6. Administración basada en funciones y perfiles de usuario, con autenticación integrada mediante inicio de sesión único (ISS).</p> <p>11.7. Capacidad de auto-monitoreo de la consola de gestión, incluyendo alertas, estados de salud y eventos del sistema.</p> <p>11.8. Asignación y administración de recursos por máquina virtual (procesador, memoria, red y almacenamiento) con políticas dinámicas de aprovisionamiento.</p> <p>11.9. Consola de administración con alta disponibilidad, desplegada en forma de dispositivo virtual (appliance virtual).</p> <p><b>Funcionalidades avanzadas:</b></p> <p>11.10. Plataforma de orquestación y automatización con herramientas integradas para análisis de registros, gestión de capacidad, cumplimiento normativo, supervisión activa y resolución de problemas (depuración).</p> <p>11.11. Motor de ciclo de vida para automatizar la instalación, configuración, actualización y corrección de componentes del entorno de virtualización (procesamiento, red, almacenamiento y gestión).</p> <p>11.12. Administración de clústeres con capacidad para realizar actualizaciones de firmware y software validadas desde la misma consola de administración.</p> <p>11.13. Soporte nativo para contenedores y orquestación de contenedores mediante Kubernetes dentro del entorno virtualizado.</p> <p>11.14. Gestión avanzada de dominios de carga de trabajo, con asignación de políticas específicas de disponibilidad y rendimiento.</p> <p><b>Seguridad:</b></p> <p>11.15. Cifrado de datos en reposo tanto para discos virtuales como para máquinas virtuales completas.</p> <p>11.16. Compatibilidad con módulos de plataforma segura (TPM 2.0) tanto físicos como virtuales.</p> <p>11.17. Control de acceso con niveles granulares, con trazabilidad y monitoreo del estado y comportamiento de los sistemas virtuales.</p> <p><b>Rendimiento y sostenibilidad:</b></p>
--	--



	<p>11.18. Soporte para aceleradores especializados como unidades de procesamiento de datos (UPD) y unidades de procesamiento gráfico (UPG), orientado a cargas de trabajo intensivas como inteligencia artificial y aprendizaje automático.</p> <p>11.19. Capacidad de distribución equilibrada de cargas considerando factores de eficiencia energética y consumo por aplicación.</p> <p>11.20. Soporte para zonas de disponibilidad y movilidad dinámica de cargas de trabajo entre dichas zonas.</p> <p><b>Integraciones e interfaces de programación (APIs):</b></p> <p>11.21. Consola de administración extensible mediante interfaces de programación de aplicaciones (API), permitiendo la integración con plataformas de terceros.</p> <p>11.22. Validación continua de los componentes físicos y virtuales dentro de clústeres a través de una matriz electrónica de compatibilidad actualizada.</p> <p>11.23. La solución debe estar clasificada como líder en el cuadrante mágico de Gartner en la categoría de virtualización de infraestructura.</p> <p>11.24. La consola de administración será entregada como un dispositivo virtual (appliance) que centralice todas las tareas de gestión.</p> <p>11.25. El hipervisor debe ejecutarse directamente sobre el núcleo del hardware, sin sistema operativo subyacente.</p> <p>11.26. Se debe contar con una plataforma de gestión unificada que integre: orquestación, supervisión, cumplimiento normativo, gestión de capacidad y resolución de problemas en una sola interfaz.</p> <p>11.27. El entorno debe permitir el uso de modo híbrido vinculado (modo vinculado híbrido), integrando entornos locales y remotos bajo una misma vista de gestión.</p> <p>11.28. La gestión del ciclo de vida debe realizarse mediante una herramienta de administración de centro de datos definido por software (Administrador SDDC), permitiendo actualizaciones validadas del conjunto completo de soluciones.</p> <p>11.29. El licenciamiento incluye servicios de instalación, configuración inicial y puesta en funcionamiento del entorno.</p> <p><b>Bases de la convocatoria:</b></p> <p>1. El Licitante que desee participar en el Servicio de actualización integral de la infraestructura tecnológica para el sitio alterno del Instituto Registral y Catastral del Estado de Nuevo León (IRCNL), deberá:</p>
--	--



	<ol style="list-style-type: none"><li>1.1. Incluir un <b>diagrama de arquitectura conceptual</b>, donde se muestren todos los componentes de la solución propuesta.</li><li>1.2. Incluir, para el componente <b>respaldo centralizado</b>, licenciamiento para respaldar servidores con los siguientes sistemas operativos: Windows, IBM, AIX y Linux, así como las versiones más recientes de dichos sistemas operativos durante la vigencia del contrato.</li><li>1.3. Presentar una carta del fabricante que asegure al menos <b>cinco (5) años de refacciones</b> para los componentes a ser suministrados.</li><li>1.4. Presentar una carta de <b>garantía</b> del fabricante, que asegure que los productos suministrados están exentos de vicios ocultos que puedan comprometer su funcionamiento y desempeño durante el período de garantía estipulado.</li><li>1.5. Presentar una carta del fabricante indicando que los <b>equipos fueron sometidos a pruebas de calidad</b>.</li><li>1.6. Presentar una carta que certifique el <b>tiempo de establecimiento</b>.</li><li>1.7. Presentar una carta que certifique la autorización del fabricante como <b>distribuidor autorizado</b>.</li><li>1.8. Presentar una carta del fabricante que certifique son <b>equipos nuevos y no discontinuados</b>.</li><li>1.9. Presentar una carta que indique las <b>normas de calidad</b>.</li><li>1.10. Presentar una carta que sobre la <b>vida útil de los equipos propuestos</b>.</li><li>1.11. Presentar una carta oficial del fabricante en la que se certifique que la cadena de suministro del fabricante implementa prácticas y medidas de control preventivas y de detección, las cuales protegen los activos físicos y minimizan el riesgo de introducción maliciosa de malware y componentes falsificados.</li><li>1.12. la autorización del fabricante como <b>distribuidor autorizado</b></li><li>1.13. Demostrar su <b>experiencia</b> para ejecutar este servicio mediante la celebración de por lo menos un (1) contratos en los últimos doce (12) meses, con</li></ol>
--	---



	<p>características iguales o similares al servicio solicitado.</p> <p>1.14. Demostrar mediante un <b>Plan de Trabajo</b>, estar en condiciones de <b>realizar y entregar el servicio en 16 semanas, o menos</b>, a partir del fallo y se incluyan las actividades específicas a realizar por cada persona, la relación entre cada actividad, los recursos, la fecha de inicio y la fecha de fin de cada actividad, los entregables y un gráfico de Gantt que muestre todas las actividades.</p> <p>1.15. Anexar un documento con el <b>Plan de Transferencia de Conocimiento</b>, buscando que, a la finalización del Servicio, el equipo de IRCNL obtenga lo descrito en la sección Especificaciones técnicas, punto diez (10). El plan podrá llevarse a cabo a la par del servicio o una vez finalizado.</p> <p>1.16. Demostrar el <b>cumplimiento de contratos</b> mediante las actas de entrega recepción de servicios de por lo menos un (1) contrato en los últimos doce (12) meses, con características iguales o similares al servicio solicitado.</p> <p>1.17. Comprometerse a que toda la <b>información</b> que le proporcione la Convocante, así como la generada durante el desarrollo del Servicio, es de carácter <b>confidencial y propiedad del Instituto Registral y Catastral del Estado de Nuevo León (IRCNL)</b> mediante la firme de un convenio de confidencialidad y exclusividad por cada empleado que forme parte del equipo de trabajo.</p> <p>1.18. Asegurar que todo el personal que participe en el Servicio firme <b>el convenio de confidencialidad y exclusividad</b> correspondiente.</p> <p>1.19. Presentar una cotización detallada donde incluya cada componente especificado en la ficha técnica.</p> <p>1.20. Ejecutar una batería completa de pruebas de funcionalidad que permita verificar el correcto desempeño, estabilidad, interoperabilidad y cumplimiento técnico de todos los componentes instalados (servidores, almacenamiento, respaldo, conmutadores, DRP y demás elementos de la infraestructura). Estas pruebas deberán realizarse una vez concluida la instalación y configuración del sistema, en presencia del personal designado por el Instituto Registral y Catastral del Estado de Nuevo León.</p>
--	--



1.21. Los siguientes componentes del servicio: Servidores físicos, almacenamiento unificado, respaldo centralizado y conmutadores de red a ser suministrados deberán ser del mismo fabricante.

1.22. Se deberán presentar garantías y soporte, indicando plazos, niveles de servicio (SLA) y atención postventa.

**Propuesta técnica:**

Dentro de un sobre cerrado, el Licitante deberá incluir lo siguiente:

1. Un documento con el **diagrama de la arquitectura conceptual** propuesta.
2. **Lista de equipos y plataformas**, incluyendo **licenciamiento**, a suministrar como parte de la arquitectura conceptual propuesta.
3. Documento con una **matriz de cumplimiento** de cada punto descrito como parte de las especificaciones técnicas de los componentes correspondientes.
4. **Ficha técnica de la licitación** indicando que cumple cada punto del servicio solicitado, las bases y entregables, como parte de su propuesta.
5. Para demostrar su **experiencia** para ejecutar este servicio, anexar copia simple y original, o copia certificada para cotejo, de los contratos celebrados con características iguales o similares al servicio solicitado.
6. Anexar un documento con el **Plan de Trabajo** donde se incluyan las actividades específicas a realizar por cada persona, la relación entre cada actividad, los recursos, la fecha de inicio y la fecha de fin de cada actividad, los entregables y un gráfico de Gantt que muestre todas las actividades.
7. Anexar un documento con el **Plan de Transferencia de Conocimiento**, buscando que, a la finalización el Servicio, el equipo de IRCNL obtenga lo descrito en la sección Especificaciones técnicas, punto diez (10).
8. Para demostrar el **cumplimiento de contratos**, anexar copia simple y original, o copia certificada para cotejo, de las Actas de entrega recepción de servicios de contratos celebrados con características iguales o similares al Servicio solicitado.



	<p>9. Anexar <b>Cartas</b> del fabricante solicitadas en las bases de esta licitación, en original y con firma autógrafa.</p>
<p><b>Entregables</b></p>	<p>El Licitante adjudicado deberá entregar:</p> <p>I. <b>Acta de entrega recepción del servicio</b>, conforme al siguiente calendario:</p> <p><b>1er Entregable - Tercer semana de iniciado el servicio</b></p> <ol style="list-style-type: none"> <li>1. Acta parcial de entrega recepción.</li> <li>2. Arquitectura de la solución (diagrama físico y lógico).</li> </ol> <p><b>2do Entregable - Séptima semana de iniciado el servicio</b></p> <ol style="list-style-type: none"> <li>3. Acta parcial de entrega recepción.</li> <li>4. El Plan de trabajo con porcentaje de avance, asignación de recursos, y fecha de inicio y fin.</li> <li>5. Especificaciones técnicas de equipos y software a ser suministrado.</li> </ol> <p><b>3er Entregable - Onceava semana de iniciado el servicio</b></p> <ol style="list-style-type: none"> <li>6. Acta parcial de entrega recepción.</li> <li>7. Suministro de cada componente.</li> <li>8. Evidencia fotográfica.</li> </ol> <p><b>4to Entregable - Décima sexta semana de iniciado el servicio, sin exceder el 18 de noviembre del 2025.</b></p> <ol style="list-style-type: none"> <li>9. Acta final de entrega recepción.</li> <li>10. Manual de usuario (operación básica y administración).</li> <li>11. Manual de soporte técnico y procedimientos de escalamiento.</li> <li>12. Manual de configuración de cada componente.</li> <li>13. Manual de instalación paso a paso.</li> <li>14. Capacitación.</li> <li>15. Transferencia de conocimiento.</li> <li>16. Memoria Técnica.</li> <li>17. Evidencia fotográfica.</li> <li>18. Carta garantía de equipos y servicios</li> <li>19. Contactos de soporte y hoja de servicio postventa</li> </ol>



	<p>EL proveedor deberá de entregar documento con <b>garantía por 60 días sin costo</b> alguno en donde se resolverán todos aquellos detalles que pudieran presentarse en los puntos antes mencionados.</p>
--	--

<b>Términos y condiciones</b>	
<b>Tiempo de entrega</b>	<p>El servicio se ejecutará en un periodo máximo de <b>hasta 16 semanas</b>, sin exceder la fecha del <b>18 de noviembre del 2025</b>.</p> <p>El Licitante seleccionado deberá estar en condiciones de iniciar la prestación del servicio a partir del día hábil siguiente en que se haya dado el Fallo Definitivo y Adjudicación.</p>
<b>Lugar de entrega</b>	<p>Washington 2000 Oriente, Col. Obrera, 64010, Monterrey, Nuevo León. Dirección de Información del Instituto Registral y Catastral del Estado de Nuevo León (IRCNL) ubicado en el Sótano de Pabellón Ciudadano.</p>
<b>Responsable de la recepción y puesto</b>	<p>Ing. Javier Jorge Hernández Dueñas, Director de Información del Instituto Registral y Catastral del Estado de Nuevo León (IRCNL).</p>
<b>Origen del Recurso</b>	<p>Recurso propio del IRCNL.</p>
<b>Forma de pago</b>	<p>Cuatro pagos durante la vigencia del contrato, conforme a la siguiente tabla:</p> <p><b>1er pago, correspondiente al 25% del contrato</b> - Dentro de los 5 días hábiles posteriores a la <b>tercera semana</b> de iniciado el servicio. Se requiere adjuntar acta de entrega-recepción parcial del servicio, con un reporte y exposición de avance del servicio, así como la factura que reúna los requisitos fiscales.</p> <p><b>2do pago, correspondiente al 25% del contrato</b> - Dentro de los 5 días hábiles posteriores a la <b>séptima semana</b> de iniciado el servicio. Se requiere adjuntar acta de entrega-recepción parcial del servicio, con un reporte y exposición de avance del</p>



	<p>servicio, así como la factura que reúna los requisitos fiscales.</p> <p><b>3er pago, correspondiente al 25% del contrato</b> - Dentro de los 5 días hábiles posteriores a la <b>onceava semana</b> de iniciado el servicio. Se requiere adjuntar acta de entrega-recepción parcial del servicio, con un reporte y exposición de avance del servicio, así como la factura que reúna los requisitos fiscales.</p> <p><b>4to pago, correspondiente al 25% del contrato</b> - Dentro de los 5 días hábiles posteriores a la <b>décimo sexta semana</b> de iniciado el servicio. Se requiere adjuntar acta de entrega-recepción parcial del servicio, con un reporte y exposición de avance del servicio, así como la factura que reúna los requisitos fiscales.</p>
<p><b>Penalidad por incumplimiento</b></p>	<p>Será del 0.1% (cero punto un por ciento) diario, del valor de lo no entregado, por cada día de atraso.</p>
<p>"Las características técnicas son las deseables y mínimas, mas no limitativas"</p>	

