

## **ANEXO II**

**ESPECIFICAÇÕES TÉCNICAS  
ESPECIFICACIONES TÉCNICAS**

**ADITAMENTO 1  
ADITIVO 1**

VERSÃO EM ESPANHOL  
VERSIÓN EN ESPAÑOL

## 1 OBJETO

Adquisición de solución de Gerenciamiento de Acceso Privilegiado (Privileged Access Management - PAM) - **Beyond Trust**, así como servicios de implementación, migración, capacitación y soporte técnico especializado.

## 2 ALCANCE DE LA SOLUCIÓN

El alcance de la solución incluye la adquisición de licencias, productos y servicios para la implementación de la solución de Gestión de Acceso Privilegiado **Beyond Trust** en la ITAIPU, que deberá realizarse de forma única, incluyendo:

- Etapa de planificación y elaboración del proyecto ejecutivo.
- Provisión de equipos, software y licencias.
- Servicios de instalación, configuración y pruebas de campo.
- Migración de datos de la solución actual a la nueva solución.
- Acompañamiento del comisionamiento y puesta en marcha.
- Servicios de soporte técnico (Banco de Horas bajo demanda).
- Documentación.
- Capacitación.
- Integraciones con sistemas existentes (bajo demanda).
- Garantías y otros elementos y servicios necesarios para el completo y perfecto funcionamiento de la solución.

## 3. ESPECIFICACIONES DE LOS PRODUCTOS Y SERVICIOS

3.1 El CONTRATISTA deberá proveer los productos y servicios de la solución de Gestión de Acceso Privilegiado (PAM) de acuerdo con los siguientes requisitos técnicos:

- **Fabricante:** Beyond Trust.
- **Tipo de licencia:** Suscripción.
- **Tipo:** Appliance virtual y Appliance físico.
- **Período de licencia:** 36 meses.

| Artículo | PRODUCTOS Y SERVICIOS                                                                         | Unidad   | CANTIDAD |
|----------|-----------------------------------------------------------------------------------------------|----------|----------|
| 1        | Beyond Trust Password Safe                                                                    | Activos  | 2.100    |
| 2        | Beyond Trust Privileged Remote Access - PRA                                                   | Usuarios | 50       |
| 3        | Beyond Trust Workforce Password                                                               | Usuarios | 300      |
| 4        | Beyond Trust Appliance Virtual                                                                | Unidades | 2        |
| 5        | Beyond Trust Appliance Físico                                                                 | Unidades | 2        |
| 6        | Servicio de implementación y migración de datos (incluye integración de Service-Now y Splunk) | Unidad   | 1        |
| 7        | Capacitación (transferencia de conocimientos)                                                 | Unidad   | 1        |
| 8        | Soporte Técnico Local y Remoto - Banco de Horas                                               | Horas    | 900      |

Tabla 1 - Relación de productos y servicios

3.2 Las cantidades de licencias especificadas son referencias aproximadas para atender las necesidades de todo el ambiente de la ITAIPU, conforme detallado a continuación. Es responsabilidad del CONTRATISTA entregar licencias suficientes para cumplir con dicho ambiente:

- La licencia del producto "**BeyodTrust Password Safe**" deberá ser suficiente para gestionar el siguiente ambiente:
  - 1000 (mil) servidores Linux/Unix.
  - 500 (quinientos) servidores Windows.
  - 100 (cien) instancias de base de datos.
  - 500 (quinientos) activos de red (switches, routers, firewalls, controladores, balanceadores, WAF y otros).
  - 250 (doscientas cincuenta) aplicaciones web.
  - 500 (quinientos) usuarios accediendo al cofre/gateway (siendo al menos 50 simultáneamente).
- La licencia del producto "**BeyodTrust Privileged Remote Access - PRA**" deberá ser suficiente para garantizar el acceso remoto de al menos 50 accesos simultáneos.
- La licencia del producto "**BeyodTrust Workforce Passwords**" deberá ser suficiente para garantizar el uso del producto por al menos 300 usuarios.

3.3 La solución ofertada por el CONTRATISTA deberá integrarse con **Splunk SIEM** y **Service-Now ITSM**, en caso de que esta integración tenga costos o licencias específicas, estas deberán ser parte integral de la propuesta presentada por el CONTRATISTA.

3.4 La integración con Splunk SIEM y Service-Now ITSM es responsabilidad del CONTRATISTA y deberá ser ejecutada en la fase de implementación de la solución.

3.5 La solución ofertada por el CONTRATISTA deberá funcionar en modo clúster de alta disponibilidad en el modelo Activo/Pasivo, utilizando obligatoriamente Appliances Virtuales en la plataforma VMWare vSphere y Appliances físicos, tanto para el **producto BeyodTrust Password Safe** como para **BeyodTrust Privileged Remote Access - PRA**.

3.6 El CONTRATISTA deberá garantizar la actualización de versión de los softwares contratados durante la vigencia del contrato, incluyendo versiones principales (major releases), versiones secundarias (minor releases), y versiones de mantenimiento (maintenance releases) y las actualizaciones de cualquier naturaleza (updates y patches) que fueren disponibilizados para todos los softwares especificados en la sección 3.1, sin cargo adicional.

3.7 La activación de las licencias (conteo de plazos de vigencia) deberá ser solamente a partir del inicio de la implementación del producto, es decir, el período de 36 meses deberá ser contados a partir del inicio del proceso de implementación de la solución.

3.8 Los productos deberán estar certificados para el entorno tecnológico de la ITAIPU descrito en el ítem 10 Ambiente Tecnológico de la ITAIPU.

3.9 Todos los ítems de este proceso de adquisición deberán ser proporcionados por el mismo CONTRATISTA.

3.10 Para el objeto del ítem 5 de la Tabla 1 - Lista de Productos y Servicios, como alternativa al equipo integralmente de la marca BeyondTrust, será admitido el suministro de Appliance Físico implementado sobre servidor de un fabricante distinto, conforme marca y modelo indicados en la oferta comercial del CONTRATISTA (hipótesis 2.4.1.1 del PBC), debidamente dimensionado según los requisitos técnicos del fabricante BeyondTrust y con la solución preinstalada y funcional, manteniendo los demás requisitos definidos en esta especificación técnica.

3.11 En la hipótesis del suministro del hardware descrito en el ítem 3.10, es de entera responsabilidad del CONTRATISTA todo el soporte y la garantía del hardware suministrado, incluyendo, entre otras, las actualizaciones de firmware, actualizaciones del sistema operativo y sustitución de piezas o componentes, durante la vigencia del contrato, sin costo adicional para ITAIPU y sin consumir, para estas actividades, horas de "Soporte Técnico Local y Remoto - Banco de Horas".

3.12 Todos los componentes de software necesarios para el correcto funcionamiento de la solución en el hardware ofertado para actuar como "appliance físico", conforme ítem 3.10, deberán ser suministrados y mantenidos por el CONTRATISTA durante toda la vigencia del contrato.

#### 4 IMPLEMENTACIÓN Y MIGRACIÓN DE LA SOLUCIÓN ACTUAL

4.1 EL CONTRATISTA deberá realizar la planificación de actividades en conjunto con la ITAIPU, esta planificación deberá incluir las diversas tareas que se realizarán a lo largo del período de implementación y migración de datos. Esta planificación deberá quedar registrada en un cronograma que orientará su respectiva ejecución.

4.2 La instalación, personalización de la solución y migración de datos son de responsabilidad del CONTRATISTA, y deberá considerar las buenas prácticas definidas por el fabricante. Estas actividades deberán realizarse de manera presencial en las instalaciones de la Central Hidroeléctrica de Itaipú, de acuerdo con el cronograma previamente definido.

4.3 La instalación y personalización de la solución abarca la migración de la solución actual a la nueva plataforma y la integración completa de la solución con los demás elementos de la infraestructura preexistente en la ITAIPU. Los costes relacionados con esta actividad deben incluirse en la oferta de precios.

4.4 El producto actual que será migrado a la solución BeyondTrust es el "Password Manager Pro" de la empresa "ManageEngine" (PMP)  
<https://www.manageengine.com/br/passwordmanagerpro/>.

4.5 La migración deberá contemplar toda la base de activos del Password Manager Pro - PMP - que incluye sistemas MS Windows, Red Hat Linux y PostgreSQL, MSSQL y Oracle, así como las políticas de rotación de contraseñas para los activos mencionados. También hay credenciales de un solo uso (sin integración ni rotación de contraseñas) que deben migrarse.

4.6 Deberá ser migrado el Workflow de aprobación para el check-out de credenciales del sistema SAP, así como la rotación de contraseñas después del check-in de las credenciales. Esta integración con SAP se puede realizar de forma nativa, vía API o a través de un script externo.

4.7 Se deberán migrar (implementados en la solución BeyondTrust) al menos los siguientes informes:

- Informe de check-out y check-in de credenciales por grupo de activos.
- Informe de acceso remoto (PRA) y del gateway de acceso.
- Informe de Password Out of Sync.

4.8 La implementación de la solución BeyondTrust no se limita a la migración de los ítems especificados anteriormente. En la etapa de planificación ITAIPU especificará las demás funcionalidades, flujos e informes que deben incluirse en la solución implementada.

4.9 EL CONTRATISTA deberá proporcionar toda la documentación técnica, manuales, diagramas lógicos y físicos, procedimientos para el funcionamiento de los productos en medios digitales,

preferiblemente en portugués y español, excepcionalmente en inglés.

## 5 CAPACITACIÓN (TRANSFERENCIA DE CONOCIMIENTOS)

5.1 EL CONTRATISTA deberá realizar transferencia de conocimiento de la solución implementada en la Itaipú y tener una duración de hasta 40 horas para al menos 12 personas.

5.2 Es responsabilidad del CONTRATISTA la elaboración de material de apoyo (folletos) y material audiovisual para la transferencia de conocimientos.

5.3 La transferencia de conocimiento deberá ser realizada de manera presencial en las instalaciones de la ITAIPU, por un profesional capacitado del contratista o del fabricante.

5.4 La planificación de las fechas y horarios de ejecución serán acordadas entre el CONTRATISTA y la ITAIPU.

5.5 La evaluación de la capacitación será realizada por la ITAIPU. Si más del 50% de los participantes indican que no cumplieron con las expectativas esperadas, se debe repetir la capacitación.

5.6 Si la insuficiencia de la capacitación se debe a problemas en el desempeño del instructor, si así se indica en las evaluaciones, se deberá realizar otra, con la misma carga horaria y con otro instructor, sin costo adicional para la ITAIPU.

## 6 SERVICIOS DE SOPORTE TÉCNICO LOCAL Y REMOTO - BANCO DE HORAS

6.1 El alcance del soporte técnico (local y remoto) incluye actividades relacionadas con la planificación, consultoría, apoyo en proyectos internos, soporte, configuración, personalización, pruebas e implementación de las herramientas de BeyondTrust adquiridas en este documento o cualquier otro elemento relacionado con esta plataforma.

6.2 Deberán ser proveídos servicios de soporte correctivo y preventivo, con profesionales capacitados en todas las soluciones proporcionadas, y capaces de desarrollar servicio remoto y local en la oficina de la Central Hidroeléctrica de ITAIPU, en ciclos periódicos o bajo demanda, con el fin de garantizar el perfecto funcionamiento del sistema y el mantenimiento de todos los criterios de desempeño, disponibilidad y seguridad.

6.3 La presente contratación deberá contemplar un banco de horas, con 900 horas de soporte técnico local y remoto, sin garantía de facturación, que deberá ser previamente solicitado, programado y aprobado por la ITAIPU y será utilizado con los siguientes criterios para el cálculo de horas:

| Tipo de servicio                                   | Unidad | Cantidad | Equiv. |
|----------------------------------------------------|--------|----------|--------|
| Soporte técnico remoto (independiente del horario) | Hora   | 1        | 0,7    |
| Soporte on-site (horario comercial)                | Hora   | 1        | 1      |
| Soporte on-site (nocturno)                         | Hora   | 1        | 1,5    |
| Soporte on-site (fines de semana y feriados)       | Hora   | 1        | 2      |

Tabla 2 Equivalencia de horas de servicio

6.4 Para los efectos de fijación de precios de las horas, se deberá considerar el valor del soporte on-site (horario comercial), ya que las demás tienen una equivalencia en relación con este.

6.5 Las solicitudes de servicio on-site serán de al menos 24 horas por solicitud, y programadas con al menos 15 días de antelación con el CONTRATISTA.

6.6 Los gastos de traslado, alojamiento, alimentación y otros gastos de viaje son responsabilidad exclusiva del CONTRATISTA.

6.7 Para todas las actividades, tanto de Soporte Técnico como de la implementación, el CONTRATISTA deberá firmar un acuerdo de confidencialidad, en los términos presentados por la ITAIPU, con respecto a la información obtenidas sobre la Infraestructura de ITAPU.

6.8 El CONTRATISTA deberá garantizar la disponibilidad técnica y la atención de los servicios de soporte técnico remoto en régimen 24x7, para todo el conjunto de servicios que forman parte de este contrato, sin límite de accionamientos y que deberá cumplir con los requisitos de nivel de servicio especificados en la tabla 3.

| SEVERIDAD | DESCRIPCIÓN                             | INICIO DEL SERVICIO | CIERRE DEL SERVICIO |
|-----------|-----------------------------------------|---------------------|---------------------|
| 0         | Ambiente Parado                         | Inmediato           | 4 h                 |
| 1         | Funcionamiento deteriorado.             | 6 h                 | 12 h                |
| 2         | Dudas, consultas o demandas específicas | 12 h                | 24 h                |
| 3         | Actividad planificada                   | Negociado           | Negociado           |

*Tabla 3: Acuerdo de nivel de servicio (SLA) de soporte técnico remoto*

6.9 El inicio de la prestación del Soporte Técnico Remoto no podrá exceder el tiempo máximo (en horas corridas) establecido en la columna INICIO DEL SERVICIO, a partir de la apertura del llamado por parte de la ITAIPU, teniendo el CONTRATISTA hasta el tiempo máximo (en horas corridas) establecido en la columna CIERRE DEL SERVICIO para concluir las actividades de soporte, informando la efectiva solución del problema o solución de contorno.

6.10 Los niveles de severidad serán definidos por la ITAIPU en el momento de la apertura del llamado y podrá sufrir alteraciones a lo largo del servicio.

6.11 Cuando se tratare de una "Actividad Planificada", con horarios de inicio y finalización del servicio negociado, antes del inicio de la actividad, el CONTRATISTA deberá presentar el número de horas estimadas para la ejecución de la actividad, y esto deberá ser aprobado previamente por la ITAIPU antes del inicio efectivo.

6.12 En cualquier momento, caso el CONTRATISTA observe que no será posible cumplir con los plazos establecidos para el inicio y/o finalización del servicio, deberá notificar formalmente a la ITAIPU, presentando las debidas justificaciones del incumplimiento de los plazos, y corresponderá únicamente a la ITAIPU aceptar o no las justificativas presentadas.

6.13 Cuando la solución y/o respuesta pasar a depender del FABRICANTE, entrarán en vigor los tiempos de servicio y solución descritos por el FABRICANTE, considerando siempre el programa de soporte contratado por ITAIPU con el FABRICANTE.

6.14 El cierre del servicio y el cierre del llamado solamente podrán ser realizados luego de ser validados y certificados por la ITAIPU.

6.15 Solamente serán facturadas las horas del banco de horas efectivamente utilizadas, que deberán ser previamente solicitadas, programadas y aprobadas por la ITAIPU.

6.16 El servicio de soporte técnico caracterizado como SEVERIDAD 0, debe iniciarse inmediatamente después de la activación y registro del llamado, utilizando recursos de acceso remoto si necesario.

6.17 Para las actividades de Soporte Técnico Local, solo formarán parte de este cómputo las horas consumidas en las actividades designadas por la ITAIPU o en local previamente aprobado por el área gestora. No deberá formar parte de este cálculo las horas consumidas desde el traslado del técnico hasta la presentación en la ITAIPU.

6.18 En los casos de servicios de soporte técnico local, se deberá realizar un informe técnico de las actividades realizadas.

6.19 El CONTRATISTA deberá disponer de al menos DOS medios para la apertura de llamados, siendo obligatorio un canal telefónico, y el otro podrá ser correo electrónico o sistema de web de tickets.

6.20 Hasta 10 días siguientes a la fecha indicada en la OIS, el CONTRATISTA deberá realizar una reunión de planificación con la ITAIPU para definir los cronogramas de las actividades a ser realizadas.

## 7 REQUISITOS FUNCIONALES MÍNIMOS DE LA SOLUCIÓN

7.1 La solución **Beyond Trust Password Safe** debe garantizar el cumplimiento del siguiente conjunto de requisitos durante toda la vigencia del contrato:

7.1.1 Mantener la oferta y el soporte de Appliance físico para la solución.

7.1.2 Garantizar el funcionamiento de la solución on-premise, en las instalaciones de la ITAIPU, sin necesidad de recursos en la nube.

7.1.3 Mantener una solución disaster recovery nativa en el producto.

7.1.4 Mantener infraestructura simplificada a través del concepto de appliances all-in-one, donde todos los recursos necesarios para el funcionamiento de la solución están presentes en el appliance.

7.1.5 Mantener el soporte oficial, ofertado por el fabricante, a través de Brasil o Paraguay.

7.1.6 Mantener compatibilidad completa y nativa con clientes de Windows, Linux (GUI) y MacOS.

7.1.7 Mantener compatibilidad total y sin agentes con los activos administrados Windows Server, Linux Server, SGBDs.

7.1.8 Mantener soporte para la integración con los componentes Splunk SIEM y Service-Now ITSM utilizados en la ITAIPU.

7.1.9 Proveer mecanismo automatizado para grabación de sesión y registro de logs de accesos remotos realizados a través de la herramienta.

7.1.10 Permitir gestión del acceso privilegiado mediante la configuración de grupos de acceso.

7.1.11 El proveedor o usuario final no debe conocer la credencial del sistema específico al que necesita acceder.

7.1.12 La Solución debe funcionar con equipos, sistemas o dispositivos finales que se encuentren en más de un dominio o AD de Microsoft.

7.1.13 Posibilitar la configuración del acceso remoto a los sistemas en función de los siguientes criterios:

- perfil de acceso (consulta, administración, etc.).
- activo y/o sistema (conjunto de activos) a ser accedidos.
- usuario y/o grupo de usuarios (ej: área/sector responsable).
- workflow de aprobación.
- control de acceso basado en roles (RBAC).

7.1.14 Proporcionar autenticación multifactor.

7.1.15 Posibilitar la elaboración de flujos para aprobación de las solicitudes de acceso realizadas por usuarios con autorización.

7.1.16 Permitir el acompañamiento en tiempo real de la sesión remota realizada (funcionalidad "over the shoulder"), así como permitir la grabación de esta en vídeo y/o texto (teclas pulsadas) de forma automática y transparente, con el fin de garantizar mecanismos de auditoría para el acceso.

7.1.17 En caso de necesidad o emergencia, deberá ser permitido al administrador terminar la sesión remota.

7.1.18 Proveer flujos independientes de concesión de acceso para sistemas o activos que son de responsabilidad de diferentes áreas.

7.1.19 Permitir la configuración de permisos de acceso remoto vinculados a intervenciones específicas, con plazos definidos (ej: fechas previstas de inicio y finalización) a través de flujos de aprobación configurables.

7.1.20 Disponer de una interfaz de programación (API) que permita la integración de los flujos de aprobación de acceso remoto con herramientas externas para la gestión de tickets.

7.1.21 Permitir la configuración de acceso vía API.

7.1.22 Proveer controles que permitan auditoría y generen alertas cuando se realice el acceso.

7.1.23 Permitir supervisión del acceso remoto en curso, proporcionando información como:

- Activo al que se accede.
- Usuario conectado.
- Tiempo de conexión.
- Integración para enviar eventos a otros sistemas a través de APIs/Protocolos.

7.1.24 Finalización automática de sesiones basada en la inactividad de la sesión.

- 7.1.25 Permitir identificar cambios en los patrones de comportamiento de acceso de los usuarios y actuar para mitigar las infracciones.
- 7.1.26 Permitir el mapeo e identificación de los activos conectados al entorno y sus respectivas credenciales y certificados digitales.
- 7.1.27 Posibilitar el cambio automático de contraseña de forma periódica y/o después de acceder a la credencial de la bóveda.
- 7.1.28 Permitir el uso compartido seguro de contraseñas habilitando el acceso segmentado a credenciales específicas en función de los grupos de acceso.
- 7.1.29 Disponer de un mecanismo de almacenamiento centralizado y seguro de las credenciales del sistema para su uso en caso de "disaster recovery".
- 7.1.30 Permitir el almacenamiento seguro de tokens y usuario/seña de usuarios de servicio utilizados para integración de sistemas.
- 7.1.31 Permitir la elevación de privilegios de usuarios de manera administrada para acceder y ejecutar aplicaciones o servicios específicos restringidos a perfiles de administración.
- 7.2 La solución **BeyondTrust Privileged Remote Access** deberá garantizar el cumplimiento del siguiente conjunto de requisitos durante la vigencia del contrato:
- 7.2.1 Permitir acceso remoto seguro sin necesidad de una VPN, reduciendo los riesgos de exposición.
- 7.2.2 Permitir el acceso "just-in time" garantizando que los usuarios solo estén permitidos cuando sea necesario, minimizando el riesgo de acceso no autorizado.
- 7.2.3 Proporcionar un control granular y detallado sobre todas las sesiones privilegiadas, con auditoría y cumplimiento.
- 7.2.4 Garantizar la integración nativa con la solución **BeyondTrust Password Safe** evitando la duplicación de datos.
- 7.3 La solución **BeyondTrust Workforce Password** debe garantizar que se cumplan los siguientes requisitos durante la vigencia del contrato:
- 7.3.1 Soportar carpetas de seguridad personalizadas, donde cada usuario tiene carpetas individuales para sus contraseñas diarias, lo que permite a los empleados mantener sus credenciales de forma segura directamente desde el navegador.
- 7.3.2 Soporte para extensiones de navegador, asegurando la integración en los flujos de trabajo existentes de los usuarios, simplificando la recuperación de contraseñas y el autocompletado. Al menos los siguientes navegadores deben ser compatibles: Mozilla Firefox, Google Chrome y Microsoft Edge.
- 7.3.3 Poseer capacidades integrales de auditoría enfocadas en el entorno empresarial, que permitan rastrear, analizar y revisar las acciones de los usuarios.
- 7.3.4. Permitir la detección de actividades sospechosas relacionadas con el acceso a las aplicaciones comerciales de los empleados y proporcionar una visión holística del estado de las contraseñas en toda la organización.

7.3.5 Permitir la aplicación de políticas de contraseñas, asegurando que las contraseñas cumplan con las políticas de seguridad, cubriendo todas las aplicaciones, no solo las privilegiadas.

## **8. CUALIFICACIÓN TÉCNICA DE LOS PROFESIONALES**

8.1 El CONTRATISTA deberá comprobar la cualificación técnica de los profesionales que actuarán en la implementación, migración, capacitación y soporte técnico mediante la documentación correspondiente, presentando dentro de los 30 días siguientes a la fecha indicada en la Orden de Inicio del Servicio (OIS), los certificados de especialización de los profesionales involucrados en las actividades.

8.2 Los profesionales involucrados en las actividades de implementación, migración, capacitación y soporte técnico deberán comprobadamente pertenecer al personal del cuadro propio del CONTRATISTA o del FABRICANTE, debiendo ser comprobado dicha vinculación mediante la documentación adecuada dentro de los 30 días siguientes a la fecha indicada en la Orden de Inicio de Servicio (OIS).

8.3 El CONTRATISTA deberá comprobar que cuenta en su cuadro funcional con al menos 01 (un) profesional con al menos 01 (una) certificación oficial de los productos BeyondTrust relacionados con la presente contratación. Para comprobar la certificación, el CONTRATISTA deberá presentar los certificados oficiales de capacitación del fabricante, así como la documentación que acredite la relación del profesional certificado con el CONTRATISTA.

8.4 ITAIPU se reserva el derecho de no aceptar la atención de profesionales no calificados, debiendo el CONTRATISTA reemplazar inmediatamente al profesional para no comprometer el servicio final.

## **9. CONDICIONES DE SUMINISTRO Y ACEPTACIÓN**

9.1 La ITAIPU solamente emitirá la aceptación de la solución después de la debida recepción, evaluación técnica de todos los ítems incluidos en este proceso y verificación de que están de acuerdo con lo especificado.

9.2 El CONTRATISTA emitirá, junto con la facturación mensual, un informe de calidad del servicio, informando el número de llamados al soporte remoto y sus respectivos tiempos de atención en el período, comparándolos con el SLA especificado en el ítem 6.8 (Tabla 3).

9.3 El CONTRATISTA deberá presentar una comprobación del registro de los software junto al fabricante, evidenciando el debido licenciamiento y otras garantías.

9.4 El CONTRATISTA deberá presentar la comprobación de que el soporte registrado junto a BeyondTrust para los productos contratados se ajusta a una modalidad apropiada para los requisitos de esta especificación.

9.5 El CONTRATISTA es responsable por el correcto comportamiento y eficiencia de su personal, comprometiéndose a prestar los servicios con personal técnico especializado en las actividades a desarrollar con el fin de concluir eficientemente las solicitudes de servicio abiertas.

## **10. AMBIENTE TECNOLÓGICO DE ITAIPU**

10.1 Servidores de Microsoft Windows Server 2003 y superiores (32 bits y 64 bits).

10.2 Servidores Red Hat Enterprise Linux 6 y superiores (64 bits).

10.3 Plataforma de virtualización VMware ESXi 5.5 y versiones posteriores.

10.4 Desktops: Windows 7 e superiores (32-bits e 64-bits).

10.5 Microsoft 365 E3, E5, F3.

10.6 SIEM de Splunk.

10.7 Service-Now ITSM.