OPERADORA FERROVIARIA S.E. FOLIO N° 5

PLIEGO DE ESPECIFICACIONES TÉCNICAS PARTICULARES

Artículo 1°. - OBJETO

El presente documento tiene como objeto establecer las características técnicas necesarias para la adquisición de UN (1) Sofware de Proxy con Seguridad integrada a fin de ser empleados en los Centros de Cómputos (data center) de todas las SOFSE, con el objetivo de mejorar la seguridad de navegación en internet para todas las capas de infraestructura de red en todas las redes de la Operadora Ferroviaria Sociedad del Estado (SOFSE).

ALCANCE

La provisión incluye una descripción pormenorizada de la solución técnica ofrecida, la cual deberá incluir todos los detalles que permitan evaluar el cumplimiento técnico del sistema, con indicación de marca, modelo y opciones de hardware cuando corresponda.

Cabe aclarar que a lo largo del presente documento y para una mayor claridad técnica, algunos términos se han conservado en su lengua nativa o con sus acrónimos sajones.

Artículo 2°. - OFERTA TÉCNICA

Contendrá el desarrollo y descripción en forma pormenorizada de la propuesta técnica y el detalle de equipos, materiales y accesorios a utilizar.

Se integrará con:

a) Descripción técnica detallada para cada ítem ofertado.

b) La documentación en la que consten las características técnicas que forman parte de la propuesta del Oferente.

c) Antecedentes técnicos requeridos.

Artículo 3°. – PLAZO DE ENTREGA Y LUGAR DE ENTREGA

El plazo de entrega es de TREINTA (30) días corridos como máximo, a partir de la notificación de la orden de compra.

Las personas de contacto serán:

Esteban Cerutti
mail: esteban.cerutti@trenesargentinos.gob.ar

Lic. Leonel Miglioli
Gerente de Tecnología de la Información e Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

OPERADORA FERROVIARIA S.E. FOLIO N° 6

tel: 011-2150-9300 interno 26387

Baseggio Federico
mail federico.baseggio@trenesargentinos.gob.ar
tel: 011-2150-9300 interno 26437

El lugar de entrega será:

Dr. Ramos Mejía 1358 4to piso Of. Sistemas

Artículo 4°. - DESCRIPCIÓN

Especificaciones Técnicas requeridas para la provisión del sistema.

El mismos deberán cumplir con la totalidad de las siguientes características y requerimientos mínimos, con una cantidad mínima de 5000 licencias.

CARACTERÍSTICAS GENERALES

La solución ofrecida deberá ser robusta, segura y eficiente para proteger el ambiente de navegación a internet de al menos 1000 usuarios simultáneos, proporcionando las funcionalidades de:

* Proxy HTTP, HTTPS, FTP y Socks.
* Almacenamiento en caché
* Categorización y Control de URL con un mínimo de 85 categorías
* Análisis y bloqueo de URL usando el concepto de Reputación
* Control granular y Visibilidad de Aplicaciones WEB
* Filtrado de contenido
* Filtrado de contenido por cuota de tiempo y/o de volumen trazado

Debe poseer módulos de antivirus, sin la necesidad de componentes de hardware adicionales

Inspección de Tráfico SSL, sin la necesidad de componentes de hardware adicional.

Módulo de control Inspección con protección contra ataques de Malware y aplicaciones maliciosas con soporte para protección contra malware avanzado sin la necesidad de incluir equipos adicionales

La solución ofrecida deberá contar con todo el licenciamiento necesario para desplegar en una etapa inicial 5 nodos (1000 usuarios por nodo) distribuidos en las distintas líneas de Trenes y un crecimiento de hasta 10 nodos. Si para lograr esto fuere necesario agregar licenciamiento o hardware adicional, deberá proveerse dentro de la oferta base.

El soporte, actualización y mantenimiento de esta solución deberá tener vigencia por un periodo de 12 meses para todos los servicios solicitados.

CARACTERÍSTICAS DE PROXY Y CACHE

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información é Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

FEDERICO BASEGGIO
COORDINADOR TÉCNICO INFORMÁTICA
SERVICIOS REGIONALES
G.T.I.
OPERADORA FERROVIARIA S.E.

Servidor Proxy debe ser compatible para la navegación con cualquier navegador y sistema operativo

Actuar nativamente como proxy de los protocolos HTTP, HTTPS, FTP y Socks

Actuar como proxy SOCKS, con definiciones de políticas de usuarios y grupos específicos para ese protocolo.

Debe soportar como mínimo los siguientes navegadores para la gestión vía GUI:

Firefox 3 y versiones más recientes

Internet Explorer 7 y versiones más recientes (sólo Windows)

Safari 4 y versiones más recientes - (sólo Mac OS X)

Google Chorme (Comprobar versiones para incluir)

La interfaz de configuración a través de GUI debe admitir como mínimo los siguientes idiomas:

* Inglés

* Español

Soportar control FTP en HTTP (en los modos activo y pasivo)

El cliente FTP puede especificar el puerto para el control de conexión a través del siguiente formato: hostname: port

Independiente del modo de FTP cliente que el usuario utilice el FTP proxy, el primero debe intentar actuar en modo pasivo la conexión al servidor FTP. Si el servidor remoto no admite Passive Mode, el Proxy debe funcionar en modo activo.

Posibilitar la configuración del puerto o puertos utilizados para el servicio de proxy para HTTP, HTTPS, FTP y SOCKS

Posee la capacidad de utilizar el proxy con el método CONNECT para puertos tunelados en HTTP

Debe ser capaz de crear una lista de destinos que pueden omitir las reglas de proxy y las políticas basadas como mínimo en:

* Dirección IP

* CIDR

* Zona

* Hostname completo o parte.

* Grupo de usuarios

* Categorías de URL

* Puertos del proxy

El proxy proporcionado debe soportar operación tanto en modo explícito como en modo transparente. En el caso de modo transparente, debe implementarse la redirección de conexiones a través del protocolo WCCPv2

El servicio de proxy debe funcionar para IPv4 e IPv6 - en modo transparente y explícito.

Posee integración con servicios de directorio LDAP y dominios Windows para auditoría y autenticación sin la necesidad de instalación de agentes o plugins en ninguna estación de trabajo o servidor

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

La solución debe hacer la autenticación del usuario vía NTLM de modo transparente, es decir, utilizando usuario ya autenticado en dominio Windows sin solicitar nuevamente la contraseña para el usuario.

El equipo debe solicitar autenticación (login, contraseña y dominio) para usuarios que utilizan sistemas operativos diferentes de Windows (Linux, por ejemplo), validando estos usuarios en el servicio de directorios de Microsoft Active Directory y LDAP.

La solución debe ser compatible con el estándar de seguridad de la firma de nombres de la versión 2 (SAMLv2)

La solución debe tener la capacidad de funcionar como un proveedor de identidad en entornos con SAML, creando, manteniendo y administrando información de identidad y proporcionando dicha información a los proveedores de servicios.

Debe ser posible a un usuario con perfil de administrador acceder, desde un equipo de otro usuario, sitios y recursos que no estén disponibles para tal usuario con menor privilegio.

Deberá permitir la re-autenticación, donde un usuario con perfil de administrador pueda acceder a determinados sitios / recursos de una máquina de otro usuario que no tenga el perfil de acceso

Deberá permitir la creación de políticas con un perfil de Bypass de autenticación, permitiendo que usuarios o visitantes puedan acceder a Internet con acceso limitado, por el hecho de no ser un usuario autenticado

Debe permitir la creación de políticas sofisticadas utilizando al menos los siguientes criterios:

Grupos de dominio o servicio de directorios LDAP y AD a los que pertenece el usuario

Clasificación de las páginas (categorías de URL)

* Tipos de archivo

* Puerto del servicio de proxy al que el usuario ha conectado

* Reputación del sitio de destino

* Listas de URLs registradas

* Base de URLs con contratación de actualizaciones con el proveedor

* Tipo de contenido

* Mime Type

* Presencia de malware

* Tamaño de la descarga

* Dirección IP

* Expresiones Regulares para URLs

* Expresos Regulares para objetos

El sistema debe ser capaz de alojar archivos PAC (Proxy Auto-configuration) y disponerlo a través de puertos configurables.

La solución deberá permitir la reposición del PAC existente con una nueva versión del mismo nombre, y la solución deberá preguntarse si quiere sustituir o no

Debería ser posible configurar múltiples Proxy HTTP para redirigir el tráfico si es necesario para otras capas de Proxy, posibilitando configuraciones de Failover, Equilibrio o condicional

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

[redacted]

OPERADORA FERROVIARIA S.E. FOLIO N° 9

La solución cuando se implementa con la función de proxy proxy, debe permitir que la dirección IP se especifique a través del encabezado X-forwarded-for, en lugar de tener sólo la dirección IP del proxy proxy

Debe poseer la funcionalidad de IP Spoofing (posibilitar encaminar el direccionamiento

CARACTERÍSTICAS DEL PROXY HTTPS (CRIPTOGRAFADO)

La solución deberá tener la capacidad de descifrar conexiones HTTPS, utilizando al menos los siguientes criterios:

Basado en la categoría del sitio de destino

Basado en la reputación del sitio de destino

Basado en el estado del certificado proporcionado por el sitio de destino (por ejemplo, los sitios con certificados caducados o firmados por una CA no confiable siempre se descifrar)

La solución deberá permitir la aplicación de los mismos análisis efectuados para los protocolos FTP y HTTP para el protocolo SSL / HTTPS

La solución deberá actuar como un "man in the midle", y deberá admitir certificados on-box, importando certificados válidos o generando certificados autofirmados

La solución debe soportar la funcionalidad de Solicitud de Firma de Certificación (CSR) Support - es decir, cuando se genera un certificado y la clave en la solución, debe permitir que el CSR permita ser enviado en una CA. Y después de recibir el certificado de la CA, el mismo permite subirlo a solucón y ese proceso debe ser hecho vía GUI

Debe admitir el módulo de encriptación adherido al estándar FIPS 140-2, Nivel 1.

Debe admitir el protocolo de protocolo de control de sucesos (OCSP) para comprobar en tiempo real el estado de los certificados junto a la autoridad de certificación correspondiente.

Debe permitir la administración de certificados, permitiendo la inclusión y eliminación de certificados de la lista de certificados de confianza.

Debe permitir la carga de certificados con claves privadas encriptadas, protegidas por contraseña inaccesible a los usuarios.

Debe admitir claves de certificados SSL de 2048 bits.

CARACTERÍSTICAS DEL FILTRO DE CONTENIDO WEB

El equipo debe actualizar la base de URL automáticamente a través de Internet a través de una base propietaria del fabricante del equipo

Debe poseer una base de URLs con al menos 85 categorías predefinidas, 250.000 de URL's categorizadas y 50 millones de dominios registrados

La base de URL debe poseer sitios en al menos 50 idiomas y de al menos 150 países

Debe permitir la creación de categorías extras personalizadas, sin límite, basadas como mínimo en:

* Dirección IP del servidor

Lic. Lionel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

* Subred

* Zona

* Expresiones regulares en las URL.

Debe posibilitar el envío al fabricante de las URLs no registradas en la base de datos para análisis e inclusión en la base de categorías a través del portal y del portal del fabricante

Debe permitir notificar al usuario sobre la política de uso de la empresa cuando accede a sitios prohibidos, permitiendo o no el acceso si el usuario desea continuar.

La página de notificación para el usuario deberá rastrear quién aceptó la página de "End User Acknoledgement" por sesión de la cookie o dirección IP cuando no hay un username disponible

La solución debe recordar / almacenar la información de notificación "End User Acknoledgement" incluso después de reiniciar el proxy

Posee categoría específica para sitios que puedan contener malware

Posibilidad de bloqueo de acceso a sitios de chat y foros en línea

Posee categoría específica para sitios de descarga

Posee categoría específica para sitios que tengan como objetivo la distribución de radio, video y telefonía por Internet

Debería ser capaz de crear acciones diferentes para las URL en políticas por tiempo

Deberá permitir la personalización de la página de notificaciones a los usuarios

Debe tener al menos las siguientes categorías de URL, sin costos adicionales:

* Sitios de contenido malicioso

* Sitio de chat (chat) y foros en línea

* Sitios de Filter Avoidances

* Sitios de relaciones

* Sitios de redes personales

* Sitios de acceso remoto y residencial - no permitir acceso a máquinas remotas vía URL dinámicas y que caracterizan el acceso remoto

* Sitios de pornografía (contenido adulto, pedofilia, erótico y también educación sexual)

* Sitios web y webmail corporativo (OWAs)

* Sitios de descarga y peer-to-peer (P2P)

* Sitios de streaming (audio y video en línea)

* Sitios de juegos

* Sitios de hacking.

Deberá tener filtro contra pérdida de información vía Web (HTTP y HTTPS) y FTP con el mínimo analizando los siguientes parámetros. (Ej. Funcionarios del Financiero no puede enviar arqiuvo XLS vía FTP):

* Metadata Archivo (nombre de archivo, tipo de archivo y tamaño de archivo).

* Usuario

* Grupo de usuarios (interacción AD / LDAP)

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

OPERADORA FERROVIARIA S.E. FOLIO N° 11

* URL, Categoría o Reputación.

CARACTERÍSTICAS DEL FILTRO DE REPUTACIÓN

Debe poseer un sistema de filtro de reputación que permita establecer una reputación para cada dirección IP de los servidores de destino con las siguientes características:

Debe utilizar datos de una red mundial de supervisión de tráfico para definir la reputación de los servidores de destino consultando un número mínimo de 10000 redes participantes con cobertura global

La red de reputación no sólo se basa en la información de flujo de la propia base de dispositivos instalada, sino en muchos otros parámetros procedentes de: listas negras de URL, listas blancas de URL, listas de equipos comprometidos, volumen global de tráfico, histórico de los sitios, datos de categorización de URLs y web rastreadores

Debe permitir acciones diferenciadas de acuerdo con cada reputación obtenida, como bloquear, permitir o verificar detalladamente los objetos de cada acceso

CARACTERÍSTICAS DE ANTI-MALWARE

La solución debe contener herramienta antimalware

Debe soportar el servicio de verificación de la reputación de archivos en nube, para la detección preventiva de malware avanzado

La solución deberá permitir, para los casos en que la reputación del archivo sea desconocida, el envío para análisis dinámico en "Sandbox". Este análisis puede ser realizado en nube o localmente a través de la integración con dispositivos específicos.

La solución debe permitir el seguimiento de la evolución del comportamiento del malware a los archivos examinados, alertando a los administradores de los casos en que los archivos pasan a tener un comportamiento malicioso (malware) después del análisis inicial del servicio de reputación en nube

La solución deberá poseer una base de datos, actualizada periódicamente de forma automática ya través del sitio del fabricante, que permita la detección de por lo menos 200 mil diferentes tipos de malwares

Realizar todas las comprobaciones de malware simultáneamente para cada objeto del sitio, en tiempo real, y no secuencialmente, para minimizar la latencia, sin el uso de protocolos de comunicación entre las herramientas como ICAP.

El análisis antimalware, deberá ser ejecutado en el mismo equipo, no siendo aceptadas soluciones que necesiten de equipos adicionales adicionales para la ejecución de estas funcionalidades

Debe realizar la comprobación de malware en ambos sentidos (descarga y upload)

El mecanismo de detección de malware debe reconocer códigos maliciosos al menos en las siguientes categorías:

* Adware

* Phishing

* Trojan Horse

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

CARBONE
SUPERINTENDENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

* Commercial System Monitor
* Session hijackers
* Gusano
* Keystrokes - keyloggers
* Outbreak Heuristic
* Virus.

Posibilidad de almacenar el resultado de las comprobaciones de malware en caché para minimizar la latencia

Debe tener un mecanismo de verificación de tráfico en la capa 4 del modelo OSI, permitiendo identificar estaciones de trabajo infectadas por malware en la red interna del cliente, con las siguientes características:

La supervisión de tráfico en la capa 4 debe examinar el tráfico en todos los 6535 puertos del protocolo TCP

La verificación de tráfico en la capa 4 debe ser capaz de monitorear o monitorear y bloquear el tráfico sospechoso.

Deberá estar disponible un informe de gestión de capa 4, integrado al appliance que muestra y determine los sitios y aplicaciones que se han monitoreado / bloqueado

Deberá estar disponible un informe de gestión de capa 4, integrado al appliance que muestra y determine las TOP direcciones IP que acceden a sitios con malware por puertos

FUNCIONALIDAD DE ADMINISTRACIÓN Y GERENCIA

Debe poseer interfaz de gestión vía web y línea de comando

La interfaz de línea de comandos debe ser accesible a través del protocolo SSH (Secure Shell) y tener al menos comandos equivalentes a los siguientes comandos de la interfaz de línea de comandos de Linux:

* Tcpdump
* Grep
* Tail
* Ping
* Telnet.

Debe poseer MIB propia para verificación de las informaciones de uso vía SNMP y debe posibilitar el envío de alertas administrativas utilizando e-mails

Posibilitar crear políticas de acceso a la interfaz de gestión basada en direcciones IP y / o rango de IP que puedan acceder al sistema

Debe permitir la integración con RADIUS para autenticar a los usuarios en la consola de administración de soluciones.

Se debe tener la opción de asignar todas las cuentas de RADIUS al perfil de administrador o diferentes cuentas de RADIUS a diferentes perfiles de acceso a la consola de administración de la solución.

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

La solución debería permitir la creación de múltiples servidores RADIUS para la autenticación de usuarios a la administración.

El equipo debe ofrecer la posibilidad de envío de llamada al soporte del fabricante utilizando comando interno que envíe datos sobre la configuración del equipo e informaciones de estado y logs del equipo para agilizar la atención

La solución debe permitir que los registros se configuren para ser enviados a un servidor externo basado en el tamaño del archivo o en horarios predefinidos, como de hora, hora, diario, semanal mensual, o horarios personalizados

Posibilitar soporte remoto al equipo por el fabricante a través de acceso seguro al equipo habilitado por el administrador

Debe poseer al menos tres clases de usuarios, siendo ellas administrador (con permiso de cambiar configuraciones, administrar usuarios y actualizar sistema operativo), operador (con permiso de cambiar configuraciones) e invitado (sólo acceder a información de informe y estado del equipo)

La solución debe mostrar un mensaje en la interfaz gráfica, notificando al administrador cuando existe una versión del sistema operativo más reciente disponible para descargar

La solución compuesta por dos equipos deberá funcionar con los siguientes requisitos:

Los dispositivos deben funcionar como maestro y esclavo permitiendo que las configuraciones hechas en el equipo maestro sean replicadas para el equipo esclavo, a través de salvamento y carga de archivos de configuración

Cada dispositivo debe ser capaz de soportar toda la demanda y atender todos los requisitos de este edicto, en un solo equipo.

Deberá ser compatible con SNMP Traps

Debe ser compatible con Syslog

La solución debe actualizar todos los mecanismos de cheque de forma regular y automática, efectuando la descarga de forma incremental

El administrador puede realizar manualmente las actualizaciones.

CARACTERÍSTICAS DE INFORMACIÓN

Debe poseer una interfaz web de generación de informes con información en tiempo real, integrada al equipo, con las siguientes características:

Debe permitir la exportación de los datos de los informes a CSV y PDF

Debe permitir la programación del envío de los informes por correo electrónico.

La interfaz Web de informes integrada al equipo con información en tiempo real debe tener como mínimo los siguientes informes:

* Visión del sistema
* Categorías más visitadas (10 categorías al menos)
* Usuarios con más accesos (10 usuarios, por lo menos)
* Actividades del usuario
* Detalles del usuario
* Detalles de la categoría

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

* Detalles del malware

* Monitor del filtro de reputación

* Monitor de tráfico en la capa 4 del modelo OSI

* Uso de banda

* Banda ahorrada en función de bloqueos.

La solución debe poseer una interfaz web de generación de informes para informaciones que no son de tiempo real, no necesariamente integrada al equipo appliance, con las siguientes características:

Debe permitir la exportación de los datos de los informes a CSV

Debe permitir la programación del envío de los informes por correo electrónico.

Debe permitir el almacenamiento de la información en la base de datos relacional

La interfaz de informes de información que no son de tiempo real debe tener al menos las siguientes características:

* Informe de sitios y categorías accedidos (general y por usuario)

* Informe de sitios bloqueados (general y por usuario)

* Definición de un intervalo de día y hora para los informes

* Visión del sistema

* Sitios más visitados

* Usuarios con más accesos

* Actividades del usuario

* Detalles del usuario

Artículo 5°. - SERVICIOS CONEXOS DE SOPORTE TECNICO Y MANTENIMIENTO:

Alcances:

- Deberá proveer un Servicio Técnico de Garantía, Soporte y Mantenimiento en forma on-site por un período de UN (1) años, que regirá a partir de la fecha de firma del Acta de recepción y que será aplicable a todos los elementos que integren los equipos ofertados.

- El servicio a brindar, será acorde a la importancia y calidad de las prestaciones solicitadas. Para ello, los Oferentes deberán poseer la capacidad para dar cumplimiento a las condiciones de servicio exigidas, dentro del esquema de servicio 5x8xNBD (días hábiles en horario laborable con respuesta al siguiente día hábil de solicitado el servicio), con los requerimientos definidos en las presentes Especificaciones Técnicas y con el tiempo solicitado a partir del momento en que haya sido registrada la solicitud en el Servicio Único de Llamadas del Contratista.

- Se define "El tiempo de respuesta entre el pedido de reparación y el inicio de la misma" al tiempo máximo que trascurra entre el momento en que se notifica al proveedor el mal funcionamiento del sistema y la presencia de personal técnico.

Se define "El tiempo máximo de reparación" al lapso que transcurre entre el momento en que se notificó al proveedor el mal funcionamiento del sistema y el momento en que el organismo recepción y verifica el buen funcionamiento del bien afectado.

Lic. Cohel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.

OPERADORA FERROVIARIA S.E. FOLIO Nº 15

- El Oferente garantizará que el servicio técnico será brindado por personal especializado y certificado por la empresa fabricante de los productos ofrecidos.

Todas las características aquí exigidas para el Servicio Técnico de Soporte y Mantenimiento ofrecido, deberán encontrarse operativas al día de la apertura de la presente contratación.

Artículo 6°. - REQUISITOS DE LOS BIENES OFERTADO:

Si se dejara de comercializar el bien durante el periodo entre la presentación de la Oferta y su correspondiente entrega, la empresa adjudicataria deberá reemplazar por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado. Sin costo adicional para Sofse.

Ese reemplazo deberá ser previamente autorizado por quien realice el dictamen técnico.

Artículo 7°. - REQUISITOS DEL OFERENTE:

El oferente debe acreditar experiencia para la oferta a proveer, para ello deberá:

- Acreditar documentalmente estar radicado en la República Argentina, con no menos de CINCO (5) años de antigüedad previos a la presentación de la oferta.

- Acreditar documentalmente que el oferente es canal certificado de la marca propuesta por al menos DOS (2) años.

Lic. Leonel Miglioli
Gerente de Tecnologías de la Información e Innovación
Operadora Ferroviaria S.E.

FEDERICO BABEGGIO
COORDINACIÓN DE GESTIÓN INFORMÁTICA
SERVICIOS DE LARGA DISTANCIA Y REGIONALES
G.T.I.
OPERADORA FERROVIARIA S.E.

LUCAS CARBONE
SUBGERENCIA DE GESTIÓN INFORMÁTICA
G.T.I.
OPERADORA FERROVIARIA S.E.