566

343

INFORME DE VERIFICACIÓN DE ESPECIFICACIONES TÉCNICAS DE OFERTAS

LICITACIÓN POR CONCURSO DE OFERTAS – Nº PAC 40/2019 "SISTEMA INTEGRAL DE GESTIÓN REGISTRAL ELECTRÓNICO PARA LA D.G.R.P –PLURIANUAL – AD REFERÉNDUM"ID No 366.893

En la Ciudad de Asunción, Capital de la República del Paraguay, a los seis días del mes de diciembre del año dos mil diez y nueve, en la **oficina de Evaluación de Ofertas, sito en el 4to piso, Torre Sur, de la Corte Suprema de Justicia**, se llevó a cabo la verificación de las especificaciones técnicas de las ofertas presentadas en el marco del referido llamado.

Se deja constancia que la verificación técnica fue llevada a cabo por el Lic. Hugo Rodríguez, el Lic. Jorge Pompa, Ing. Magno Ayala y el Lic. Gustavo Amarilla, en representación de la DGRP.

Conforme el Acta de Apertura de Sobres de fecha 29 de noviembre de 2019 del proceso de referencia, se recibió las ofertas de los siguientes oferentes:

1) Consorcio GDE
2) Consorcio KEDS

Habiendo verificado las ofertas, en base a las planillas de servicios y productos ofertados, los documentos relacionados, se presentan las planillas respectivas a: El cumplimiento de las EETT correspondientes al 80% como valoración del aspecto Técnico correspondiente al PAC 40/2019, indicadas en el PBC, sus adendas y aclaratorias respectivas publicadas ante el Portal de la DNCP.

Resumen de la evaluación detallada en las planillas adjuntadas: (Ambos Consorcios han obtenido más de 75 Pts. Solicitados como mínimo para su aceptación).

Consorcios	***Total de Puntos Evaluado de las ofertas (Sobre 100 Pts.)***	***Total de Porcentaje Obtenido de la Evaluación Técnica (Sobre el 80%)***
Consorcio GDE	**97 Pts.**	**77,60 %**
Consorcio KEDS	**92 Pts.**	**73,60 %**
Por tanto, el mayor porcentaje referente a la parte Técnica corresponde al Consorcio GDE con el 77,60 %.		

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno D. Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

CORTE SUPREMA DE JUSTICIA
COMITÉ DE EVALUACIÓN DE OFERTAS
MESA DE ENTRADA
06 DIC. 2019
Firma: Hora: 09:21
Aclaración: Lic. CLAUDIA VERA
Corte Suprema de Justicia
COMITÉ DE EVALUACIÓN DE OFERTAS

565

342 b,s

EVALUACIÓN PARTE TECNICA (CORRESPONDE AL 80 % DEL 100%).
EXPERIENCIA TÉCNICA

EXPERIENCIA GENERAL

Volumen de facturación de la experiencia en desarrollo e implementación de sistemas informáticos

Experiencia General	Pts	Pts Max	Consorcio GDE	Consorcio KEDS
MAS DE 6.000.000.001 en los últimos 5 (CINCO) AÑOS	10	10	10	10
G. 4.500.000.001 A 6.000.000.000 en los últimos 5 (CINCO) AÑOS	7			
G. 3.5000.000.000. a G. 4.500.000.000 en los últimos 5 (CINCO) AÑOS	3			
El oferente presenta contratos				

EXPERIENCIA ESPECÍFICA

Cantidad de Sistemas Transaccionales en entorno web realizados e implementados, durante los últimos 5 años.

Sistemas	Pts	Pts Max	Consorcio GDE	Consorcio KEDS
7 o más Sistemas Transaccionales en entorno web	15	15	15	15
4 a 6 Sistemas Transaccionales en entorno web	10			
1 a 3 Sistema Transaccionales en entorno web	5			
El oferente presenta contratos				

Experiencia en desarrollo de sistemas informáticos que vinculen e indexen documentos digitalizados.

Cantidad	Pts	Pts Max	Consorcio GDE	Consorcio KEDS
Desarrollo de sistemas que vinculen e indexen documentos. DESDE 1.500.001 documentos digitalizados.	15	15	15	15
Desarrollo de sistemas que vinculen e indexen documentos. DESDE 500.001 HASTA 1.500.000 documentos digitalizados.	10			
Desarrollo de sistemas que vinculen e indexen documentos. Hasta 500.000 documentos digitalizados.	5			
El oferente presenta contratos				

Normas y Certificaciones

Cantidad	Pts	Pts Max	Consorcio GDE	Consorcio KEDS
CMMI y/o ISO	6	10	10	10
Certificado PMI – Gerente de Proyecto	4			
Presenta certificación CMMI y/o ISO de la empresa			6	6
Presenta certificado PMI del Gerente de Proyecto			4	4

Propuesta Técnica

Propuesta	Pts	Pts Max	Consorcio GDE	Consorcio KEDS
Plan de Trabajo y Detalle de los productos	1	3	3	3
Cronograma de actividades	1			
Descripción de los objetivos estratégicos y Programa de acción	1			
Reducción de plazos en el cronograma de actividades	2	2	2	2
Total Posible		5	5	5
Presenta a) Plan de Trabajo y El detalle de los productos				
Presenta b) El cronograma de actividades				
Presenta c) La descripción de los objetivos estratégicos y El programa de acción				
Presenta propuesta que agrega valor a los TDRs				

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno D. Ayala R.
Jefe de Div. Aplicaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

Graciela G.B.
Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

564

EVALUACIÓN DEL PLANTEL TECNICO

GERENTE DE PROYECTOS/LÍDER

Requerimientos	Pts	P. Max. Individual	Consorcio GDE	Consorcio KEDS
Experiencia Profesional, mínima de 5 años	2	10	10	5
Maestría / Doctorado	3			
Experiencia Gestión de Proyectos	3			
Experiencia Registral 1 año o mas	2			
TÍTULO UNIVERSITARIO: En Ingeniería o Licenciatura en Informática, Abogado, Escribano/Notario o profesional universitario en áreas afines al proyecto (Excluyente)				
Experiencia Profesional: Mínima de 5 (cinco) años de experiencia de haber culminado la carrera de grado			2	2
Maestría / Doctorado.			3	0
Experiencia en Gestión de Proyectos: Mínimo 2 (dos) proyectos informáticos de desarrollo de sistemas. Como Líder, Gerente, Jefe o Coordinador de proyectos de desarrollo de Sistemas en organizaciones públicas o privadas.			3	3
Experiencia Registral: 1 (un) año de trabajo para una Institución Registral.			2	0

CONSULTOR REGISTRAL

Requerimientos	Pts	P. Max. Individual	Consorcio GDE	Consorcio KEDS
Experiencia Profesional, mínima de 4 años	1	5	3	2
Maestría / Doctorado	2			
Experiencia Profesional Registral	2			
TÍTULO UNIVERSITARIO: Abogado, Escribano/Notario (Excluyente).				
Experiencia Profesional: Mínima de 4 (cuatro) años de experiencia de haber culminado la carrera de grado			1	1
Maestría / Doctorado.			0	0
Experiencia Profesional Registral: Mínimo de 3 (tres) años de experiencia comprobable como Consultor en Derecho Registral/Notarial en organizaciones públicas o asesoramiento a privados en proyectos registrales.			2	1

Obs: * 1

ESPECIALISTA FUNCIONAL O DE PROCESOS

Requerimientos	Pts	P. Max. Individual	Consorcio GDE	Consorcio KEDS
Experiencia Profesional, mínima de 3 años	1	5	5	5
Maestría / Doctorado	2			
Experiencia específica, mínima de 3 años	2			
TITULO UNIVERSITARIO: Licenciatura en Administración de Empresas o Ingeniería Comercial o Ingeniería Informática o Licenciatura en Análisis de Sistemas o Abogado o Escribano/Notario (Excluyente).				
Experiencia Profesional: Mínima de 3 (tres) años de experiencia de haber culminado la carrera de grado			1	1
Maestría / Doctorado.			2	2
Experiencia específica: Mínimo de 3 (tres) años de experiencia comprobable en O&M, o especialista de procesos, o especialista funcional en equipos de trabajo en implementaciones de sistemas de información en organizaciones públicas o privadas.			2	2

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Rompa
Jefe de Dpto.
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

563

342

JEFE DE DESARROLLO/PROGRAMACIÓN

Requerimiento	Pts	Pts Max Individual	Consorcio GDE	Consorcio WEBS
Experiencia Profesional, mínima de 3 años	3	5	5	5
Certificación en Lenguaje de servicios web	2			
TÍTULO UNIVERSITARIO: Ingeniería Informática, Licenciatura en Análisis de Sistemas o afines (Excluyente).				
Experiencia Profesional: Mínima 3 (tres) años de experiencia siendo jefe de desarrollo de software en entorno Web, con experiencia comprobable de haber desempeñado funciones en proyectos de análisis y/o diseño y/o construcción y/o desarrollo de sistemas de información, en organizaciones públicas o privadas			3	3
Certificación: en lenguajes orientados a servicios web JavaScript, PHP, HTML5, CS3. Se otorgara un punto por cada certificado. Máximo 2 puntos.			2	2

DISEÑADOR GRAFICO

Requerimiento	Pts	Pts Max Individual	Consorcio GDE	Consorcio WEBS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado curso de diseño de Interface de Sistemas de Información	1			
TÍTULO UNIVERSITARIO: Licenciatura como Diseñador Gráfico o afines, Licenciatura en Análisis de Sistemas, Ingeniero de Sistemas. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en Diseño Gráfico o Interfaces Humanas, en organizaciones públicas o privadas			1	1
Certificación: De haber realizados curso de diseño de Interface de Sistemas de Información.			1	1

ANALISTA 1

Requerimiento	Pts	Pts Max Individual	Consorcio GDE	Consorcio WEBS
Experiencia Profesional, mínima de 3 años	2	3	3	3
Posgrados afines a la labor profesional solicitada	1			
TÍTULO UNIVERSITARIO: Profesional en las carreras de Ingeniería en Informática, Análisis de Sistemas o carreras afines. (Excluyente)				
Experiencia Profesional: Mínima 3 (tres) años de experiencia en desarrollo de software en entorno Web, con experiencia comprobable de haber desempeñado funciones en proyectos de análisis y/o diseño y/o construcción y/o desarrollo de sistemas de información, en organizaciones públicas o privadas			2	2
Diplomado o Posgrados: Posgrados relacionados con Tecnología de la Información.			1	1

ANALISTA 2

Requerimiento	Pts	Pts Max Individual	Consorcio GDE	Consorcio WEBS
Experiencia Profesional, mínima de 3 años	2	3	2	3
Posgrados afines a la labor profesional solicitada	1			
TÍTULO UNIVERSITARIO: Profesional en las carreras de Ingeniería en Informática, Análisis de Sistemas o carreras afines. (Excluyente)				
Experiencia Profesional: Mínima 3 (tres) años de experiencia en desarrollo de software en entorno Web, con experiencia comprobable de haber desempeñado funciones en proyectos de análisis y/o diseño y/o construcción y/o desarrollo de sistemas de información, en organizaciones públicas o privadas			2	2
Diplomado o Posgrados: Posgrados relacionados con Tecnología de la Información.			0	1

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno O. Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

562

PROGRAMADOR 1

Requerimientos	PS	P. Max. Individual	Consorcio GDE	Consorcio KERS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado de capacitación en lenguajes de Programación Web	1			
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en desarrollo de aplicaciones similares a las definidas en las especificaciones técnicas del presente documento, en organizaciones públicas o privadas.			1	1
Certificación: Cursos en lenguajes de programación Web.			1	1

PROGRAMADOR 2

Requerimientos	PS	P. Max. Individual	Consorcio GDE	Consorcio KERS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado de capacitación en lenguajes de Programación Web	1			
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en desarrollo de aplicaciones similares a las definidas en las especificaciones técnicas del presente documento, en organizaciones públicas o privadas.			1	1
Certificación: Cursos en lenguajes de programación Web.			1	1

PROGRAMADOR 3

Requerimientos	PS	P. Max. Individual	Consorcio GDE	Consorcio KERS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado de capacitación en lenguajes de Programación Web	1			
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en desarrollo de aplicaciones similares a las definidas en las especificaciones técnicas del presente documento, en organizaciones públicas o privadas.			1	1
Certificación: Cursos en lenguajes de programación Web.			1	1

PROGRAMADOR 4

Requerimientos	PS	P. Max. Individual	Consorcio GDE	Consorcio KERS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado de capacitación en lenguajes de Programación Web	1			
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en desarrollo de aplicaciones similares a las definidas en las especificaciones técnicas del presente documento, en organizaciones públicas o privadas.			1	1
Certificación: Cursos en lenguajes de programación Web.			1	1

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Marcelo D. Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

561-

341

PROGRAMADOR 5

Requerimiento	[illegible]	[illegible]	[illegible] SDE	[illegible] KEDS
Experiencia Profesional, mínima de 2 años	1	2	2	2
Certificado de capacitación en lenguajes de Programación Web	1			
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 (dos) años de experiencia en desarrollo de aplicaciones similares a las definidas en las especificaciones técnicas del presente documento, en organizaciones públicas o privadas.			1	1
Certificación: Cursos en lenguajes de programación Web.			1	1

CONTROL DE CALIDAD (FUNCIONAMIENTO DEL SISTEMA)

Requerimiento	[illegible]	[illegible]	[illegible] SDE	[illegible] KEDS
Experiencia Profesional, mínima de 2 años	2	2	2	2
TÍTULO UNIVERSITARIO: Profesional o estudiante de últimos 2 (dos) años en las carreras de Ingeniería en Informática, Análisis de Sistemas, Desarrollador o carreras afines. (Excluyente).				
Experiencia Profesional: Mínima 2 años de experiencia en la planificación y ejecución de pruebas de ejecución correcta o automática para el control de cambios en el sistema, pruebas de caja negra y caja blanca, en proyectos de desarrollo de sistemas de información, en organizaciones públicas o privadas.			2	2
TOTAL PUNTOS POR OFERENTE----------->			**97**	**92**

Formula para hallar el porcentaje Técnico, correspondiente al 80 % del 100 posible.		
Pt x 0.80	**77,60%**	**73,60%**

Observación de Realiza Referente a:
*** 1** Se pide experiencia comprobable como Consultor en Derecho Registral/Notarial en organizaciones públicas o asesoramiento a privados en proyectos registrales, sin embargo presenta experiencia en gestión u operativa registral (por lo que se le asigna 1 punto al personal presentado por Consorcio KEDS).

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno D. Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

ANEXO I – Balanceador de carga

Cantidad		2 (Dos equipos)	Mínimo Exigido	Consorcio GDE Indicar: Cumple – No Cumple	Consorcio KEDS Indicar: Cumple – No Cumple
Marca	Cantidad			2	2
Modelo	Marca			F5	F5
	Modelo			IP 4800	IP 4800
Procedencia	Procedencia			USA	USA
1. CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO	1. CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO	El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado "appliance".	Exigido	Cumple	Cumple
		El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.	Exigido	Cumple	Cumple
		Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado.	Exigido	Cumple	Cumple
		Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en cluster virtual de múltiples equipos.	Exigido	Cumple	Cumple
		Cada equipo debe cumplir con las siguientes características: La solución debe soportar un Throughput en L7 de al menos 19 Gbps. La cantidad máxima de conexiones concurrentes L4 debe ser de al menos 27 millones. La solución debe soportar al menos 440.000 conexiones por segundo L4. La solución debe soportar al menos 1.9 millones de requests por segundo HTTP.	Exigido	Cumple	Cumple
		Cada equipo debe contar con al menos las siguientes Interfaces de red: Debe contar con al menos 8 puertos SFP (compatibles con módulos SFPs cobre, SX y LX) y al menos 4 puertos SFP+ (compatibles con módulos SR y LR).	Exigido	Cumple	Cumple
		Cada equipo debe contar con fuentes de poder redundantes AC, entradas de 220 volts	Exigido	Cumple	Cumple
		Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.	Exigido	Cumple	Cumple
		Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual.	Exigido	Cumple	Cumple
		Cada equipo debe incluir al menos 32 GB de Memoria RAM	Exigido	Cumple	Cumple
		Cada equipo debe incluir mínimo discos duro con capacidad de 450 GB de almacenamiento.	Exigido	Cumple	Cumple
		Debe soportar cluster Activo/Activo y Activo/Pasivo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).	Exigido	Cumple	Cumple
		La solución debe permitir configurar cluster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda.	Exigido	Cumple	Cumple
		Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.	Exigido	Cumple	Cumple
		Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.	Exigido	Cumple	Cumple
FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO		La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.	Exigido	Cumple	Cumple
		La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.	Exigido	Cumple	Cumple
		La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.	Exigido	Cumple	Cumple
		La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.	Exigido	Cumple	Cumple
		Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones	Exigido	Cumple	Cumple
		La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting: Round Robin Proporcional (Ratio) Proporcional dinámico Respuesta más rápida Conexiones mínimas Menor número de sesiones Tendencia de menor cantidad de conexiones Tendencia de desempeño	Exigido	Cumple	Cumple
		Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM	Exigido	Cumple	Cumple
		El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)	Exigido	Cumple	Cumple
		El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.	Exigido	Cumple	Cumple
		La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica	Exigido	Cumple	Cumple

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
...nologías de la Información

Ing. Magno B. Ayala B.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

ANEXO I – Balanceador de carga

	2. FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO	La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de: Ping. Chequeo a nivel de TCP y UDP a puertos específicos Monitoreo http y https Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft. Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. Ejecución de scripts para determinar la respuesta emulando un cliente. Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma Monitoreo de aplicaciones de mercado: LDAP FTP SMTP IMAP/POP3 Oracle MSSQL MySQL RADIUS SIP Protocolo SASP SOAP WMI SNMP	Exigido	Cumple	Cumple
		Debe poder realizar todos estos métodos de persistencia de las conexiones (afinidad): Dirección IP origen Dirección IP destino Cookies Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia Sesiones SSL Microsoft Remote Desktop	Exigido	Cumple	Cumple
		Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.	Exigido	Cumple	Cumple
		Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.	Exigido	Cumple	Cumple
		El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.	Exigido	Cumple	Cumple
		Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.	Exigido	Cumple	Cumple
		Soporte de REST API	Exigido	Cumple	Cumple
		Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.	Exigido	Cumple	Cumple
		Debe soportar el protocolo TDS para balanceo de MSSQL	Exigido	Cumple	Cumple
		Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT	Exigido	Cumple	Cumple
		El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.	Exigido	Cumple	Cumple
		La solución debe permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código.	Exigido	Cumple	Cumple
		El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3	Exigido	Cumple	Cumple
		Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).	Exigido	Cumple	Cumple
FUNCIONES DE SEGURIDAD		Cada equipo debe soportar seguridad SSL con las siguientes características: Incluir mínimo 18.000 Transacciones por segundo SSL. Soportar al menos 15 Gbps SSL Bulk Encryption (Thoughput SSL).	Exigido	Cumple	Cumple
		La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL	Exigido	Cumple	Cumple
		El Stack TLS del equipo debe soportar las siguientes funcionalidades/características Session ID Session Ticket OCSP Stapling (on line certificate status protocol) Dynamic Record Sizing ALPN (Application Layer Protocol Negotiation) Forward Secrecy	Exigido	Cumple	Cumple
		La solucion debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)	Exigido	Cumple	Cumple
		Debe soportar algoritmos de cifrado Camellia	Exigido	Cumple	Cumple
		El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall)	Exigido	Cumple	Cumple
		El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall	Exigido	Cumple	Cumple
	3. FUNCIONES DE SEGURIDAD	Firmado criptográfico de cookies para verificar su integridad	Exigido	Cumple	Cumple
		Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto) Luna.	Exigido	Cumple	Cumple

Lic. Gustavo O. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Mario D. Ayala
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

ANEXO I – Balanceador de carga

		La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.	Exigido	Cumple	Cumple
		Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.	Exigido	Cumple	Cumple
		Debe soportar HSTS (HTTP Strict Transport Security)	Exigido	Cumple	Cumple
		Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías. Scanners Exploits Windows Denial of Service Proxies de Phishing Botnets Proxies anónimos	Exigido	Cumple	Cumple
FUNCIONES DE ACELERACIÓN DE TRÁFICO	4. FUNCIONES DE ACELERACIÓN DE TRÁFICO	La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: Memoria cache. Compresión tráfico HTTP Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores	Exigido	Cumple	Cumple
		El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.	Exigido	Cumple	Cumple
		Debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.	Exigido	Cumple	Cumple
		Permitir la modificación de los headers de cache para objetos del sitio web, pudiendo respetar los headers generados por el Web server o modificarlos	Exigido	Cumple	Cumple
		Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP	Exigido	Cumple	Cumple
FUNCIONES DE FIREWALL DE APLICACIONES WEB	5. FUNCIONES DE FIREWALL DE APLICAICONES WEB	La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante)	Exigido	Cumple	Cumple
		El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall	Exigido	Cumple	Cumple
		La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.	Exigido	Cumple	Cumple
		Debe trabajar en un esquema proxy TCP reverso y/o transparente	Exigido	Cumple	Cumple
		Debe soportar la creación automática de políticas	Exigido	Cumple	Cumple
		Debe trabajar con políticas de seguridad por capas, donde se configura una política de seguridad base y las políticas de seguridad hijas heredan sus configuraciones y permita que solo cambios específicos se apliquen a las políticas hijas.	Exigido	Cumple	Cumple
		La creación automática de políticas deberá unificar múltiples URLs explícitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.	Exigido	Cumple	Cumple
		Debe trabajar en modo de bloqueo o en modo informativo	Exigido	Cumple	Cumple
		Debe permitir diferentes políticas de seguridad para diferentes aplicaciones	Exigido	Cumple	Cumple
		Debe permitir la creación de firmas personalizadas	Exigido	Cumple	Cumple
		Debe trabajar con modelos de seguridad positiva y negativa	Exigido	Cumple	Cumple
		Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana	Exigido	Cumple	Cumple
		Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.	Exigido	Cumple	Cumple
		El WAF debe permitir personalizar las páginas de bloqueo	Exigido	Cumple	Cumple
		Debe prevenir exponer el "OS fingerprinting"	Exigido	Cumple	Cumple
		Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.	Exigido	Cumple	Cumple
		El WAF Debe soportar: Restringir protocolo y versión utilizada Multi-byte language encoding Validar URL-encoded characters Restringir la longitud del método de request Restringir la longitud del URI solicitado Restringir el número de Encabezados (headers) Restringir la longitud del nombre de los encabezados Restringir la longitud del valor de los encabezados Restringir la longitud del cuerpo (body) de la solicitud Restringir la longitud del nombre y el valor de las cookies Restringir el número de cookies Restringir la longitud del nombre y valor de los parámetros Restringir el número de parámetros	Exigido	Cumple	Cumple
		El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)	Exigido	Cumple	Cumple
		El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP	Exigido	Cumple	Cumple
		El WAF debe incluir protección contra Web Scraping	Exigido	Cumple	Cumple
		Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario	Exigido	Cumple	Cumple
		Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario	Exigido	Cumple	Cumple
		Debe permitir el enmascaramiento de información sensible filtrada por el servidor	Exigido	Cumple	Cumple
		Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.	Exigido	Cumple	Cumple
		Debe permitir la integración con servidores Antivirus por medio del protocolo ICAP	Exigido	Cumple	Cumple
		Debe brindar reportes respecto a la normativa PCI DSS 2.0	Exigido	Cumple	Cumple
		Debe integrarse con Firewall de Base de Datos: Oracle Database Firewall Microsoft IBM InfoSphere Guardium	Exigido	Cumple	Cumple
		Debe proteger contra ataque DoS /DDoS de Capa 7	Exigido	Cumple	Cumple
		Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa	Exigido	Cumple	Cumple
		En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.	Exigido	Cumple	Cumple
		Debe soportar tecnologías AJAX y JSON	Exigido	Cumple	Cumple

Lic. Gustavo D. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Mario D. Ayala R.
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Graciela
Asesor
Tecnologías de

Lic. Jorge Pampa
Jefe de Dpto.
Departamento de TIC/DGRP

ANEXO I – Balanceador de carga

		Debe proteger como mínimo: Ataques de Fuerza Bruta Cross-site scripting (XSS) Cross Site Request Forgery SQL injection Parameter and HPP tampering Sensitive information leakage Session highjacking Buffer overflows Cookie manipulation Various encoding attacks Broken access control Forceful browsing Hidden fields manipulation Request smuggling XML bombs/DoS Open Redirect	Exigido	Cumple	Cumple
		Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.	Exigido	Cumple	Cumple
		Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP	Exigido	Cumple	Cumple
		Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas	Exigido	Cumple	Cumple
		Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.	Exigido	Cumple	Cumple
		Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.	Exigido	Cumple	Cumple
		Debe ofrecer protección sobre tráfico basado en WebSockets	Exigido	Cumple	Cumple
		El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo	Exigido	Cumple	Cumple
		La funcionalidad de protección contra ataques DDoS para aplicaciones debe incluir protección basada en comportamientos (Behavioral)	Exigido	Cumple	Cumple
ESTANDARES DE RED	6. ESTANDARES DE RED	Soporte VLAN 802.1q, Vlan tagging	Exigido	Cumple	Cumple
		Soporte de 802.3ad para definición de múltiples troncales	Exigido	Cumple	Cumple
		Soporte de NAT, SNAT	Exigido	Cumple	Cumple
		Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.	Exigido	Cumple	Cumple
		Soporte de Rate Shapping.	Exigido	Cumple	Cumple
		Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.	Exigido	Cumple	Cumple
		Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.	Exigido	Cumple	Cumple
		Debe soportar el protocol de OVSDB (Open vSwitch Database) para crear tuneles VXLAN usando un controlador SDN	Exigido	Cumple	Cumple
		Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS	Exigido	Cumple	Cumple
ADMINISTRACIÓN DEL SISTEMA	7. ADMINISTRACIÓN DEL SISTEMA	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)	Exigido	Cumple	Cumple
		La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.	Exigido	Cumple	Cumple
		La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.	Exigido	Cumple	Cumple
		La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.	Exigido	Cumple	Cumple
		La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales	Exigido	Cumple	Cumple
		La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: Protocolo SysLog Notificación vía SMTP SNMP versión 2.0 o superior.	Exigido	Cumple	Cumple
		El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.	Exigido	Cumple	Cumple
		El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.	Exigido	Cumple	Cumple
		La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real	Exigido	Cumple	Cumple
		Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.	Exigido	Cumple	Cumple
		Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej., Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.	Exigido	Cumple	Cumple
OTROS REQUERIMIENTOS	8. OTROS REQUERIMIENTOS	Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 36 meses. Deben poseer soporte local en modalidad 8x5 con al menos 1 técnico certificados por el fabricante o su distribuidor oficial para Paraguay	Exigido	Cumple	Cumple
		El oferente deberá facilitar números telefónicos de urgencia, direcciones de correo, y una página Web para proceder a la comunicación del problema.	Exigido	Cumple	Cumple
		El oferente deberá contar con una plataforma; propia o tercerizada, de un Centro de Manejo de incidentes, encargada de la gestión de los servicios de casos generados, de tal manera a permitir una mayor flexibilidad y consolidación de alarmas y eventos, logrando que los incidentes generados sean clasificados, asignados y registrados. El Centro de Manejo de Incidentes deberá tener capacidad de operar en modalidad 24 x 7 x 365. Para poder acceder al servicio del Centro de Manejo de Servicios deberá disponibilizar al menos 3 (tres) modalidades: • Teléfono (0800) • Mail • Web	Exigido	Cumple	Cumple
		Curso de capacitación en el uso del equipo y herramientas para dos técnicos (en la DGRP), de al menos 60 horas		Cumple	Cumple
		El oferente deberá realizar todas las tareas de instalación física y configuración del equipamiento ofertado, a fin de lograr la integración con los equipos existentes	Exigido	Cumple	Cumple
		De manera a garantizar la calidad, el oferente deberá contar con certificación ISO 9001:2015 o similar para la comercialización, diseño, y despliegue de soluciones de Tecnologías de la Información y las Comunicaciones.	Exigido	Cumple	Cumple

Lic. Gustavo G. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Mario D. [illegible]
Jefe de Div. Operaciones
Departamento de TIC/DGRP

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.G.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP

338

ANEXO II – Hardware Security Module (Módulo de Seguridad Hardware)

Cantidad	[illegible]	[illegible]	Consorcio GDE	Consorcio KEDS
Funcionalidad general	Deben proveer funciones seguras de generación, resguardo, uso, gestión, migración y administración de claves en los dispositivos HSM. Deben implementarse para el proyecto todas las funciones necesarias de protección, respaldo, replicación y recuperación segura de claves.	Exigido	Cumple	Cumple
Certificación	Deben poseer Certificación FIPS 2 nivel 3.	Exigido	Cumple	Cumple
Homologación	Deben estar Homologados por el MIC como módulo de seguridad por hardware para ser utilizado como dispositivo para custodia de claves privadas de certificados digitales del tipo F1 y F2 para realizar firmas digitales reconocidas dentro de la PKI Paraguay.	Exigido	Cumple	Cumple
Características	El clúster de HSMs debe operar en Alta Disponibilidad en modo Activo-Activo.	Exigido	Cumple	Cumple
	La generación de claves de los certificados se debe realizar exclusivamente internamente en los HSMs del conjunto.	Exigido	Cumple	Cumple
	La custodia de los certificados con alta disponibilidad se debe realizar de tal forma que sus claves solo puedan utilizarse dentro de los HSMs del conjunto.	Exigido	Cumple	Cumple
	En el clúster deben incluirse todos los componentes necesarios a nivel de hardware y software para incorporar balanceo de carga automático o configurable de forma manual. De esta forma se distribuye la atención de solicitudes de servicio y su procesamiento entre los diferentes nodos del clúster de HSMs.	Exigido	Cumple	Cumple
	Cada HSM debe soportar a diferentes factores de autenticación con quórums del tipo "k de n". El sistema podrá utilizar claves protegidas por contraseña y por tarjetas con PIN que son asignadas a un número "n" de custodios.	Exigido	Cumple	Cumple
	Los HSMs deben soportar los siguientes algoritmos: Algoritmos asimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph) Algoritmos simétricos: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES Hashing y digest de mensajes: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160 Curvas elípticas: ECC Suite B, incluyendo Brainpool y curvas customizadas		Cumple	Cumple
	Deben Incluirse las librerías de interfases que soporten los protocolos estándares o lenguajes de programación: PKCS#11 OpenSSL Java (JCE) Microsoft CAPI y CNG	Exigido	Cumple	Cumple
	Debe Incluirse la posibilidad de agregar una interfaz adicional del tipo servicios web para acceder a funciones criptográficos de los HSM vía Web Services basados en tecnología SOAP ó REST.	Exigido	Cumple	Cumple
	Debe Incluir la documentación técnica de todas las funciones disponibles para cada una de las interfases disponibles y para sus configuraciones, así como los comandos y herramientas de administración y operación.	Exigido	Cumple	Cumple
	Cada HSM debe ser provisto con rieles para alojar en un rack de 19' de 1U	Exigido	Cumple	Cumple
	Debe Poseer un teclado propio y controles en un panel integrado en el mismo dispositivo. El acceso a los mismos es protegido con mecanismos genéricos para operaciones básicas del grupo de operación autorizado más factores de autenticación multifactor individuales.	Exigido	Cumple	Cumple
	Deben poseer redundancia interna para fuente de alimentación con posibilidad de recambio hotswap y de ventilación/refrigeración.	Exigido	Cumple	Cumple
	Deben tener separación de roles de administración y operación. Y tener la capacidad de utilizar mecanismos de autorización diferentes para administradores y operadores, los cuales tienen acceso a diferentes tareas en cada HSM.	Exigido	Cumple	Cumple
	Los administradores no pueden operar claves. Las claves pueden ser asignadas a custodios (operadores tituales) que las pueden operar, por ejemplo crear o activar.	Exigido	Cumple	Cumple
	Debe poseer la posibilidad de expandir la funcionalidad de los HSM para que puedan ser Administrados y Operados en forma remota. Explicar la funcionalidad y componentes necesarios.	Exigido	Cumple	Cumple

Lic. Graciela Gil Bosco
Asesora
Tecnologías de la Información

Lic. Gustavo D. Amarilla
Jefe de Div. Redes y Comunicaciones
Departamento de TIC/DGRP

Ing. Magno D. Ayala
Jefe de Div. Operaciones y Soporte
Departamento de TIC/DGRP

Lic. HUGO RODRIGUEZ S.
Coordinador Administrativo
D.E.R.P.

Lic. Jorge Pompa
Jefe de Dpto.
Departamento de TIC/DGRP