TETÃ VIRU MOHENDAPY
MINISTERIO DE HACIENDA

MINISTERIO DE HACIENDA
ORDEN DE SERVICIO 60/2019
Fecha de Emisión 12/02/2019 - TRIPLICADO

TETÃ REKUÁI GOBIERNO NACIONAL

CONTRATO NRO. 51/2018 - CONTRATACIÓN DE SERVICIOS PROFESIONALES PARA EL MANTENIMIENTO Y CONFIGURACIÓN DEL SERVIDOR ANTIVIRUS DE LA DGIC DEL MH			
PROVEEDOR	OLAM SRL	**RUC**	80013217-3
DIRECCION	PROF. F. CHAVEZ Nº 189 C/R. ODRIOZOLA		
TELEFONO / E-MAIL	605929 / manfredo@olam.com.py		
Estimaremos se sirva (n) proveer los materiales mas abajo descriptos, según contrato Nro. 51/2018.-			
SOLICITANTE	MINISTERIO DE HACIENDA	**CDP**	79/19
LUGAR DE ENTREGA	MINISTERIO DE HACIENDA	**PAC**	345272
PLAZO DE ENTREGA		**CC**	CO-12006-18-160201
MODALIDAD	Concurso de Ofertas		

SUBSECRETARIA DE ESTADO DE ADMINISTRACION FINANCIERA

Cant.	Cant. (Letras)	Descripción del/los Bienes y/o Servicios	Unid. Medida	Presentación	valor Unit.	Total
1	UNO	SERVICIO DE MANTENIMIENTO Y CONFIGURACIÓN DEL SERVIDOR ANTIVIRUS DE LA DGIC PAGO 01/12. 5% del Valor del Contrato.	UNIDAD	EVENTO	9.200.000	9.200.000

RECIBIDO C.R.A.
Por: Alfio Alejandro Benitez
Firma: Área de Gestión Documental C.R.A. - D.A. Ministerio de Hacienda
Fecha: Hora:

DIRECCIÓN ADMINISTRATIVA RECIBIDO 19 FEB 2019 CRA Nº Coordinación RECURSOS ADMINISTRATIVOS

RECIBIDO
Por: Joel Delvalle
Firma:
Fecha: 14 FEB 2019 Hora: 14:35

TOTAL	9.200.000

SON GUARANÍES: NUEVE MILLONES DOSCIENTOS MIL.-

OBSERVACION: SIME 1726/2019. MEMO COTIC/DST 002/2019. PAGO 01/12. 5% DEL VALOR DEL CONTRATO CONFORME AL PBC.

Gerardo Barrientos Técnico Analista de Procesos Dpto. de Procesos - UOC - M.H		ECON. CHRISTIAN OCAMPOS Jefe Interino Dpto. de Procesos - UOC - M.H.	ABOG. ANDRÉS SORIA Coordinador Interino Coord. Unidad Operativa de Contratación	
ELABORADO POR	REVISADO POR	DPTO. PROCESOS UOC	COORDINACION U.O.C.	PRESUPUESTO

- Reporte de riesgos y ataques de red detectados y mitigados.
- Recomendaciones finales.

13. MODALIDAD DE PAGO

El pago se realizará en base a los productos esperados e informes de trabajos realizados los cuales serán entregados a los treinta (30) días de recepcionada las Órdenes de Servicio por parte del proveedor conforme al siguiente cuadro:

% contrato	Fecha	Documento Requerido
5%	A los treinta (30) días de la recepción de Orden de Servicio 01/12 por parte del Proveedor	Informe Inicial: Aprobado. Este documento debe incluir todos los informes, y documentaciones solicitadas en el Plan de Entregas.
5%	A los treinta (30) días de la recepción de Orden de Servicio 02/12 por parte del Proveedor	2°. informe mensual: Aprobado
5%	A los treinta (30) días de la recepción de Orden de Servicio 03/12 por parte del Proveedor	3°. informe mensual: Aprobado
5%	A los treinta (30) días de la recepción de Orden de Servicio 04/12 por parte del Proveedor	4°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 05/12 por parte del Proveedor	5°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 06/12 por parte del Proveedor	6°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 07/12 por parte del Proveedor	7°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 08/12 por parte del Proveedor	8°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 09/12 por parte del Proveedor	9°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 10/12 por parte del Proveedor	10°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 11/12 por parte del Proveedor	11°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 12/12 por parte del Proveedor	Informe Final: Aprobado. Este documento debe incluir todos los informes, y documentaciones solicitadas en el Plan de Entregas

OBS:

- **La DGIC solicitará la emisión de las órdenes de servicios desde la fecha del contrato de forma mensual.**
- **Todos los pagos se realizarán a los 60 días de presentado la solicitud de pago.**

REPUBLICA DEL PARAGUAY

MINISTERIO DE HACIENDA

SIME

Nº: 1726 AÑO: 2019

RECURRENTE: DIRECCION GRAL. DE INFORMATICA Y COMUNICACIONES

OBJETO: ELEVA INFORME S/CONTRATO

CTO.051/18 - SOLICITUD EMISION ORDEN DE SERVICIO Y/O COMPRA - OLAM S.R.L.

Subsecretaría de Estado de Administración Financiera
Dirección General de Informática y Comunicaciones
Coordinación de Operaciones de TIC
Departamento de Soporte Técnico

MEMORANDUM COTIC/DST 002/2019

LIC. JUAN CARLOS FERREIRA, ENCARGADO DE DESPACHO
DIRECCION GENERAL DE INFORMÁTICA Y COMUNICACIONES

LIC. DELIA PANIAGUA, JEFA
DEPARTAMENTO DE SOPORTE TÉCNICO

LIC. PEDRO ECHEVERRIA, TÉCNICO
DEPARTAMENTO DE SOPORTE TÉCNICO

FECHA : *10/01/2019*

REFERENCIA: *Conformidad del servicio* *Recurrente: OLAM*

Con relación a la referencia, la Empresa OLAM remite el informe de los servicios realizados del llamado LCO 08/2018 "***Servicios Profesionales para Mantenimiento y Configuración de Servidor Antivirus ID Nº: 345.272*** - Contrato M.H. N° 51/2018 correspondiente al mes de SETIEMBRE 2.018. A continuación se expone cuanto sigue:

ANTECEDENTES

En el siguiente cuadro se presenta el detalle del proceso licitatorio:

N°	Descripción	Detalle
1	PROCESO LICITATORIO	LCO 08/2018 "***Servicios Profesionales para mantenimiento y configuración de servidor antivirus ID Nº: 345.272***
2	CONTRATO	Contrato M.H. N° 51/2018
3	EMPRESA ADJUDICADA	OLAM

DOCUMENTACIÓN ENTREGADA

Se adjuntan los siguientes documentos:

N°	Documento
1	**Ordenes de Servicio OLAM N°**: 38857, 38861, 38863, 38865, 38869, 38871, 38875, 38876, 38877, 38880 - Original
2	Planilla de Asistencia Mensual – Original
3	Informe Inicial de Servicios (1/12)
4	Verificación e Informe del servidor Symantec Endpoint Protection ;Manager

Luisa González
Asist. Adm. COTIC
DGIC

2905

Subsecretaría de Estado de Administración Financiera
Dirección General de Informática y Comunicaciones
Coordinación de Operaciones de TIC
Departamento de Soporte Técnico

CONFORMIDAD DE SERVICIOS Y SOLICITUD DE EMISIÓN DE ORDEN DE SERVICIO

La documentación entregada por la empresa cumple con lo requerido y se solicita la emisión de la Orden de Servicio conforme lo establecido en el PBC y lo acordado con la UOC respecto al procedimiento para la emisión de la Orden de Servicio posterior a la realización de los trabajos, a efectos de regularización.

Se sugiere la remisión del presente informe a la Dirección Administrativa para proseguir con los trámites correspondientes.

Atentamente,

Vo. Bo.

Lic. Derlis Samudio
Encargado de Despacho Res Nº: 02/19
Coordinación de Operaciones de TIC

CC: Diosnel Acosta, Secretaría Administrativa

3 TRES

ORDEN DE SERVICIO

USO INTERNO

Nº 0038857

www.olam.com

OLAM S.R.L.

FECHA: 03/Setiembre/2018
HORA DE INICIO: 09:00h.
HORA DE FINALIZACIÓN: 12:00h.

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14. Se ejecuta tarea de actualización de contenidos. Se procede a actualizar las consolas de administración del SEPMH4 y SEPMH5 de versión 14.1 a la versión 14.2.760.0000

RESULTADOS – Quedan actualizadas las consolas, se continuará con los trabajos.

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC
CLIENTE

TECNICO
Luis Alderete

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 - 24/05/2018 * GH. * Cel.: (0981) 969 017

4ejemplo

ORDEN DE SERVICIO

USO INTERNO

Nº 0038861

www.olam.com

OLAM S.R.L.

FECHA: 05 | Setiembre | 2018

HORA DE INICIO: 09:00hs.

HORA DE FINALIZACIÓN: 12:00hs.

DATOS DEL CLIENTE

NOMBRE: Ministerio de Hacienda.

DIRECCIÓN:

RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14; se procede a crear los nuevos paquetes instaladores de SEP 14.2.760.0000 y es copiada a la gente de DGIC. Se procede a crear en todos los grupos la tarea de upgrade de la herramienta para los equipos clientes, los cuales migraron de 14.1 a 14.2.760.000

RESULTADOS – Se continuará con los trabajos.

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC

CLIENTE

TECNICO
Luis Nuñez

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

Scuveo

OLAM S.R.L.
www.olam.com

ORDEN DE SERVICIO
USO INTERNO

Nº 0038863

FECHA: 07/Setiembre/2018
HORA DE INICIO: 08:30h.
HORA DE FINALIZACIÓN: 12:00h

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14, se procede a instalar por remoto SEP 14.2 en el grupo DGPNC en Directorio y Setea y Funcionamiento Habilitados.

RESULTADOS – Se continuará con los trabajos

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC
CLIENTE

TECNICO
Luis Núñez

6SETS

OLAM S.R.L.
www.olam.com

ORDEN DE SERVICIO
USO INTERNO

Nº 0038865

FECHA: 12/ Setiembre/ 2018
HORA DE INICIO: 08:30hs
HORA DE FINALIZACIÓN: 12:00hs.

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: TEL.: FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14. Se procede a instalar los upgrade de versión 14.2.760.0000 en los clientes SEP.

RESULTADOS – Se continuará con los trabajos.

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC
CLIENTE

TECNICO
Luis Núñez

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 - 3/Agosto/2018 - GH. - Cel.: (0981) 969 017

7 siete

ORDEN DE SERVICIO

USO INTERNO

Nº 0038869

FECHA: 14 / Setiembre / 2018
HORA DE INICIO: 09:00 hs.
HORA DE FINALIZACIÓN: 12:00 hs.

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: TEL.: FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SBPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SBPM14. Se crean selección de expros en bot y se procede a actualizar cliente 14.0 a versión 14.2.760.000

RESULTADOS – Se continúan con los trabajos.

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC

CLIENTE

TECNICO
Luis Navas.

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 - 3/Agosto/2018 - GH. - Cel.: (0961) 969 017

8 DEHO

ORDEN DE SERVICIO

USO INTERNO

Nº 0038871

OLAM S.R.L. www.olam.com

FECHA: 17/ Setiembre/2018
HORA DE INICIO: 09:00hs
HORA DE FINALIZACIÓN: 12:00hs

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: TEL.: FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SOPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SOPM 14. Se ejecuta tarea de actualización de cliente SEP, de versión 14.0 a versión 14.2.760.0000

RESULTADOS – Se continúan con los trabajos.

Beatriz Villalba
Técnico
Dpto. Soporte Técnico - DGIC
CLIENTE

TÉCNICO
Luis Nuñez

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

9 mes

ORDEN DE SERVICIO

USO INTERNO

Nº 0038875

OLAM S.R.L. www.olam.com

FECHA: 21/Setiembre/2018
HORA DE INICIO: 09:00hs.
HORA DE FINALIZACIÓN: 12:00hs.

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda.
DIRECCIÓN:
RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SPM 14. Las tareas de actualización automática de versión 14.2.760.0000 son detenidas para que los clientes no reinicien de forma automática.

RESULTADOS – Se continúa con los trabajos.

CLIENTE — Pedro Estevez

TECNICO — Luis Nuñez

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

103162

ORDEN DE SERVICIO

USO INTERNO

Nº 0038876

OLAM S.R.L. www.olam.com

FECHA: 24/Setiembre/2018
HORA DE INICIO: 13:00hs
HORA DE FINALIZACIÓN: 16:30hs

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14. Se restea contraseña administrador de Pedro Echeverría; se procede a cargar licencias nuevas y generaciones en la consola de administración; se crea lista detallada de equipos que aun poseen versión SEP 12.

RESULTADOS – Se continuará con los trabajos

CLIENTE Pedro Echeverría

TECNICO Luis Ruiz

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

11 OWEE

ORDEN DE SERVICIO

USO INTERNO

Nº 0038877

www.olam.com

OLAM S.R.L.

FECHA: 26 | Setiembre | 2018

HORA DE INICIO: 08:30h.

HORA DE FINALIZACIÓN: 12:00h.

DATOS DEL CLIENTE

NOMBRE: Ministerio de Hacienda.

DIRECCIÓN:

RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SEPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SEPM 14; se envía tarea de actualización de contenidos para los equipos administrados; se mueven equipos instalados que estaban en Grupo Predeterminado al grupo que le corresponde

RESULTADOS – Se continuará con los trabajos

CLIENTE

TECNICO

Luis Ñamo

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

12 DOCE

ORDEN DE SERVICIO

USO INTERNO

Nº 0038880

www.olam.com

OLAM S.R.L.

FECHA: 28 | Setiembre | 2018
HORA DE INICIO: 08:30hs.
HORA DE FINALIZACIÓN: 12:00hs.

DATOS DEL CLIENTE
NOMBRE: Ministerio de Hacienda
DIRECCIÓN:
RUC: | TEL.: | FAX:

DESCRIPCIÓN DEL PROBLEMA – Verificación de consola SOPM 14.

TRABAJOS REALIZADOS – Se procede a verificar consola SOPM 14. Se trabaja sobre actualización de equipos D263; C946; D25; D129; D166 a versión 14.2.760.000; también se quitan print screen para preparación de informe.

RESULTADOS – Se continuará con los trabajos.

CLIENTE

TECNICO
Luis Nuñez.

30 Tal. 50/3 - Nº del 0038.001 al 0039.500 * 3/Agosto/2018 * GH. * Cel.: (0981) 969 017

								MES:	SEPTIEMBRE_2018

PLANILLA DE ASISTENCIA

Licitacion por Concurso de Ofertas
Nº 08/2018
Ministerio de Hacienda
"Servicios Profesionales para Mantenimiento y Configuracion del Servidor Antivirus"
Orden de Servicio M.H. Nº _____/2018

Nº	Fecha	Hora(Inicio)	Hora (Final)	NOMBRE Y APELLIDO	Nº DE SERVICIO	TELEFONO	CORREO ELECT.	FIRMA	ACLARACION DE FIRMA
1	03/09/18	09:00	12:00	Luis Nuñez	38.857	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
2	05/09/18	09:00	12:00	Luis Nuñez	38.861	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
3	07/09/18	08:30	12:00	Luis Nuñez	38.863	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez
4	12/09/18	08:30	12:00	Luis Nuñez	38.865	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
5	14/09/18	09:00	12:00	Luis Nuñez	38.869	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
6	17/09/18	09:00	12:00	Luis Nuñez	38.871	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
7	21/09/18	09:00	12:00	Luis Nuñez	38.875	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
8	24/09/18	13:00	16:30	Luis Nuñez	38.876	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
9	26/09/18	08:30	12:00	Luis Nuñez	38.877	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
10	28/09/18	08:30	12:00	Luis Nuñez	38.880	0974733458	luis@dam.com.py	[illegible]	Luis Nuñez.
11									
12									
13									
14									
15									

13 Tres

Microsoft KASPERSKY eset SAMSUNG IBM UniFi hp SHARP GFi OLAM Symantec. Barracuda VEEAM NetSupport ManageEngine Polycom COMODO redhat FORTINET

Asunción; 07 de enero de 2019

Señores
Ministerio de Hacienda
Sr. Juan Carlos Ferreira
REF: Contrato MH N° 51/2018

Por medio de la presente, solicitamos la recepción de Informes correspondiente a los Servicios Profesionales para Mantenimiento y Configuración del Servidor Antivirus, Informe inicial mes 1/12 (Setiembre 2018) y la correspondiente emisión de la orden de Servicios para dar continuidad a los trámites administrativos.

A tal efecto remitimos detalle de horas de soporte realizadas, con el Informe Inicial.-

Sin otro particular le saluda atentamente;

Carlos Herrera
Dpto. Licitaciones

DIRECCION GENERAL
RECIBIDO
07 ENE. 2019
Dirección General
Informática y
Comunicaciones

Lic. Nilda Giménez
Encargada Mesa de Entrada
DGIC

Dirección: Aviadores del Chaco 2462 Edificio Aura, Piso 7 – Tel.: 595 21 601 929 – Asunción, Paraguay
www.olam.com – licitaciones@olam.com.py
/OLAMSRL - /OLAMSRL

01
15 Quince

Descripción General de Symantec Endpoint Protection Manager

Cliente:

Ministerio de Hacienda

Setiembre 2018

Luis Nuñez.

Carlos Herrera
Dpto. Licitaciones

1 INTRODUCCIÓN

La descripción general de protección de Symantec Endpoint Protection Manager proporciona una evaluación de su implementación de Symantec Endpoint Protection Manager actual. El servicio apunta a un administrador de Symantec SEPM y a la base de datos correspondiente. Una utilidad de recopilación de datos obtuvo datos que incluyen estas áreas:

- Información de sistema operativo y hardware
- Configuración general y opciones

Carlos Herrera
Dpto. Licitaciones

Contenido

INTRODUCCIÓN ..... ¡Error! Marcador no definido.
1. Verificacion e informe del servidor SEPM 4
1.1 Situación del servidor de dominio del Ministerio de Hacienda 4
1.2 Servidor Base Consola Symantec Endpoint Manager 4
1.3 Configuración General y Opciones 5
2. Verificación e informe de instalación 5
2.1 Estado de integridad de conexión de los equipos 5
2.2 Políticas implementadas 6
2.3 Estado de replicación de servidores 12
2.4 Ultimas actualizaciones de los componentes de SEP 14
3. Implementación de ajustes de acuerdo a recomendaciones 17
3.1 Actualización de políticas 17
3.2 Reglas 17
3.3 Alertas y últimas versiones disponibles 17
3.4 Revisiones y pruebas de restauracion de backups 20
4. Reporte de riesgos y ataques de red detectados y mitigados 20
5. Recomendaciones 27

Carlos Herrera
Dpto. Licitaciones

1 Verificación e informe del servidor Symantec Endpoint Protección Manager

1.1 Situación del servidor de dominio del Ministerio de Hacienda:

El servidor de dominio principal del Ministerio de Hacienda es el equipo DCMH1.

1.2 Servidor Base Consola Symantec Endpoint Manager:

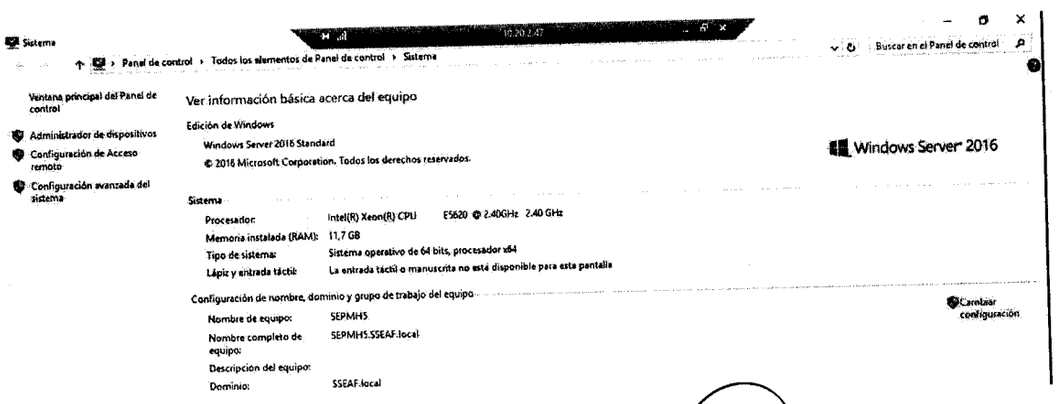
Actualmente existen dos equipos en modo de replicación que hacen de servidores para la consola Symantec Endpoint Protection Manager, son dos equipos virtuales que cuentan con Windows Server 2016 Standard x64 en español como sistema operativo base, con 12 GB de RAM, 250 DE disco, dichos servidores cuentan con dos procesadores.
El servidor primario tiene por nombre "SEPMH5", con base de datos local, la misma esta replicada en un servidor de contingencia.

CPU: Intel ® Xenon ® CPU 2.4Ghz

RAM: 11.7GB

Tipo de Sistema: Sistema Operativo Windows Server 2016 Std 64bits

Nombre de equipo: SEPMH5



Carlos Herrera
Dpto. Licitaciones

1.3 Configuración General y Opciones

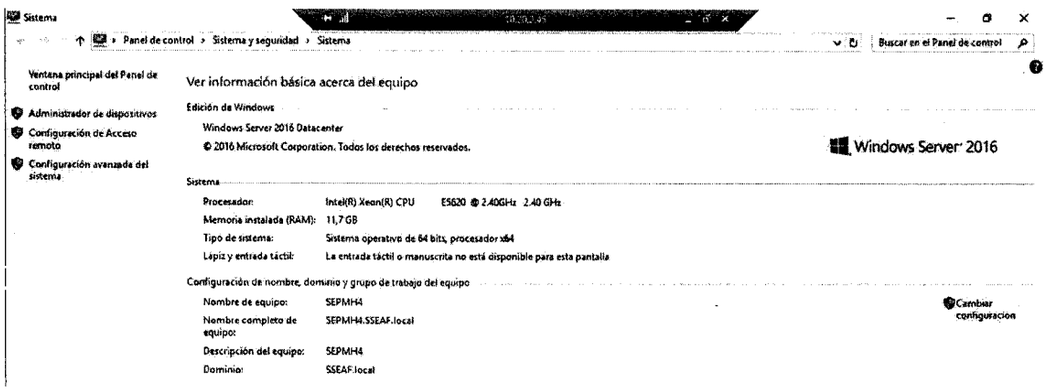
El servidor secundario lleva por nombre de **SEPMH4 y** tiene una base de datos local para el SEPM de replicación.

CPU: Intel ® Xenon ® CPU 2.4Ghz

RAM: 11.7GB

Tipo de Sistema: Sistema Operativo Windows Server 2016 Std 64bits

Nombre de equipo: SEPMH4



2 Verificación e informe de instalación

2.1 Estado de integridad de conexión de los equipos

A continuación, se detalla el estado de la conexión de los equipos clientes por dependencias:

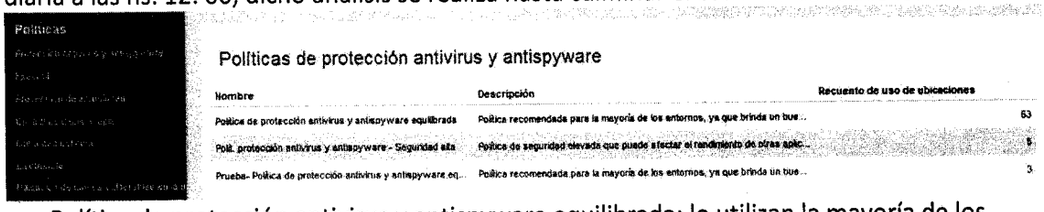
Grupo	Número de equipos
Dir. General de Informática y Comunicaciones\Funcionario Habilitado	53
Dir. General de Presupuesto\Funcionario Habilitado	46
Dir. De Pensiones No Contributivas\Funcionarios Bloqueados	41
Dirección General de Contabilidad Publica\Funcionario Habilitado	34
Dirección General de Tesoro Público\Funcionario Bloqueado	29
Dir. General de Jubilaciones y Pensiones\Funcionarios Bloqueados	26
Dirección General de Tesoro Público\Funcionario Habilitado	26
Dir. De Pensiones No Contributivas\Funcionarios Habilitado	28
Dir. General de Jubilaciones y Pensiones\Funcionarios Habilitado	22
Unidad de Departamentos y Municipios\Funcionario Habilitado	19
Dir. Gral. De Admin. de Serv. Pers. y Bienes del Estado\Funcionarios Habilit.	20
Vice Ministro\Usuario Habilitado	20
Dirección General de Jubilaciones y Pensiones\Director y Jefes	10
Dirección General de Presupuesto\Director y Jefes	7
Dirección General de Crédito y Deuda Publica\Funcionario Bloqueado	8

2.2 Políticas implementadas

Se detallan las políticas implementadas:

Virus and Spyware Protection:

Esta política está con 5 configuraciones diferentes, la misma se utilizan para que en él se realice un escaneo completo a todas las carpetas, todos los archivos incluidos con una programación diaria a las hs. 12: 00, dicho análisis se realiza hasta culminar el escaneo de todos los archivos.



a- Política de protección antivirus y antispyware equilibrada: lo utilizan la mayoría de los grupos, basada en una protección media.

b- Política de protección antivirus y antispyware-Seguridad Alta: está asociada al grupo Equipos en cuarentena Deshabilitados-DGIC-AULA y Habilitados -DGIC-AULA. Tiene una configuración más agresiva, pues en este grupo, los equipos son utilizados por muchos usuarios tanto internos como externos y conectan distintos dispositivos (USB) y es un riesgo de infección.

c- Política Protección antivirus y antispyware- Alto Rendimiento: La política está por default, y es utilizado en entornos donde no se necesita alta seguridad.

Las acciones configuradas ante la deteccion de amenazas o software malicioso son las siguientes.

- Limpiar riesgo.
- Poner riesgo en cuarentena.

En esta politica para los clientes tenemos activas las siguientes caracterisiticas o tecnologia de porteccion del clientes:

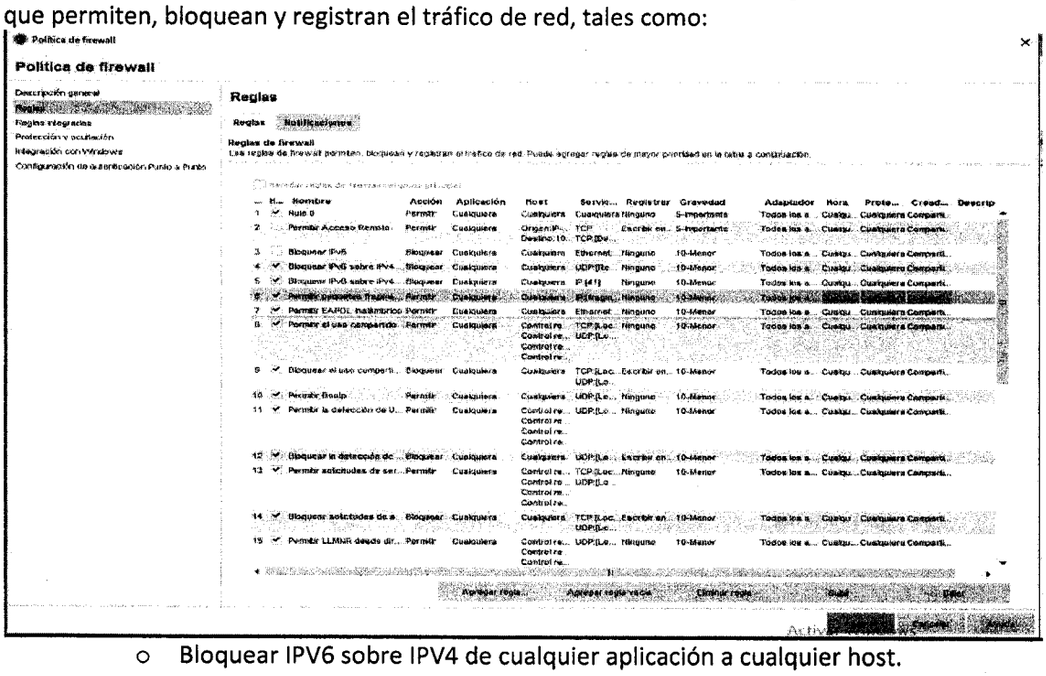
- Auto-protec.
- Proteccion de descargas.
- Sonar
- Inicio prematuro de Software malicionso.
- Analisis de correo.

Dichas caracterisitcas mencionadas mas arriba nos dan una proteccion en tiempo real del equipo que es administrado con el clientes Symantec Enpoint Protection.

Carlos Herrera
Dpto. Licitaciones

Firewall

Esta política es creada automáticamente durante la instalación, el mismo suple al Firewall de Windows deshabilitándolo. En dicho firewall el Ministerio de Hacienda tiene configuradas un total de 28 reglas que permiten, bloquean y registran el tráfico de red, tales como:



- Bloquear IPV6 sobre IPV4 de cualquier aplicación a cualquier host.
- Bloquear IPv6 sobre IPv4 (ISATAP) de cualquier aplicación a cualquier punto.
- Permitir paquetes Fragmentados.
- Permitir EAPOL inalámbrico.
- Permitir el uso compartido de archivos locales en direcciones IP privadas.
- Bloquear el uso compartido de archivos.
- Permitir Bootp.
- Permitir la detección de UPnP desde direcciones IP privadas.
- Bloquear la detección de UPnP.
- Permitir solicitudes de servicios web desde direcciones IP Privadas.
- Bloquear solicitudes de servicio web.
- Permitir LLMNR desde direcciones IP privadas (permitidas).
- Permitir LLMNR de trafico IPv6.
- Permitir detección de Servicios web desde direcciones IP privadas (permitidas).
- Bloquear detección de servicios web desde direcciones no permitidas.
- Permitir SSDP desde direcciones IP Privadas.
- Bloquear SSDP desde direcciones no permitidas.
- Permitir ping, pong y tracert.
- Permitir todas las aplicaciones.
- Permitir VPN

Carlos Herrera
Dpto. Licitaciones

- Permitir protocolos veritas.
- Permitir trafico IGMP.
- Bloquear tráfico de difusión y multidifusión y no registrar.
- Bloquear el tráfico restante de IP y registrar.
- Bloquear el tráfico restante y no registrar.

Además, contamos con dos políticas que no se encuentran habilitadas, y son las siguientes:

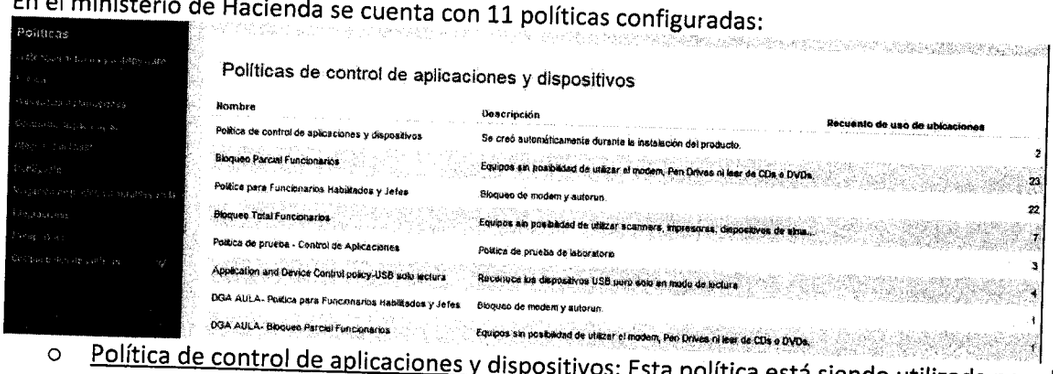
- Permitir Acceso remoto.
- Bloquear IPV6

Prevención de intrusiones.

Esta política está configurada para detector y bloquear automáticamente los ataques a nivel de red. Esta característica de prevención se creó automáticamente durante la instalación del producto, el mismo también detecta y bloquea automáticamente los ataques del navegador. Dentro de esta política tenemos asignado el rango 10.20.2.x excluida de la prevención de intrusiones.

Control de disp. y aplicaciones.

En el ministerio de Hacienda se cuenta con 11 políticas configuradas:



Nombre	Descripción	Recuento de uso de ubicaciones
Política de control de aplicaciones y dispositivos	Se creó automáticamente durante la instalación del producto.	2
Bloqueo Parcial Funcionarios	Equipos sin posibilidad de utilizar el modem, Pen Drives ni leer de CDs o DVDs.	23
Política para Funcionarios Habilitados y Jefes	Bloqueo de modem y autorun.	22
Bloqueo Total Funcionarios	Equipos sin posibilidad de utilizar scanners, impresoras, dispositivos de alma...	7
Política de prueba - Control de Aplicaciones	Política de prueba de laboratorio	3
Application and Device Control policy-USB solo lectura	Reconoce los dispositivos USB pero solo en modo de lectura	4
DGA AULA- Política para Funcionarios Habilitados y Jefes	Bloqueo de modem y autorun.	1
DGA AULA- Bloqueo Parcial Funcionarios	Equipos sin posibilidad de utilizar el modem, Pen Drives ni leer de CDs o DVDs.	1

- Política de control de aplicaciones y dispositivos: Esta política está siendo utilizada por el grupo Móvil externos (Portátiles), bloquea el acceso al autorun, bloquea la ejecución de aplicaciones, Teamviewer, AnyDesk, VNC, Dropbox, GoogleDrive, OneDrive y Spotify.
- Bloqueo Parcial Funcionarios: Esta política está configurada para que los equipos clientes no puedan utilizar modem, dispositivos de almacenamiento externo, dispositivo USB, unidades CDs o DVDs. Dicha política solo permite el acceso de los dispositivos de interfaces Humana (Teclado, Mouse) y dispositivos de impresión(Impresoras). También dentro de la política se encuentra configurada el bloqueo de aplicaciones tales como:
  - Bloquea la ejecución de programas desde unidades externas.
  - Hacer que todas las unidades sean de solo lectura.

- Bloquear escritura en unidades USB.
- Bloquear modificaciones de HOST.
- Bloquear acceso de Autorun.inf.
- Bloquea inicio de aplicaciones y extensiones .exe como Teamviewer, AnyDesk, VNC, OneDrive, GoolgeDrive, etc.

- Política para funciones Habilitados y Jefes: Esta política está configurada para que los equipos clientes no puedan utilizar modem. Dicha política solo permite el acceso de los dispositivos con excepción al modem. También dentro de la política se encuentra configurada el bloqueo de aplicaciones tales como:
  - Bloquea la ejecución de programas desde unidades externas.
  - Bloquear modificaciones de HOST.
  - Bloquear acceso de Autorun.inf.
- Bloqueo Total Funcionarios: Esta política está configurada para que los equipos clientes no puedan utilizar scanner, impresoras, dispositivos de almacenamiento externo, dispositivo USB. Además:
  - Dicha política solo permite el acceso de los dispositivos de interfaces Humana (Teclado, Mouse).
  - Bloquea la ejecución de programas desde unidades externas. Hace que todas las unidades sean de solo lectura.
  - Bloquear escritura en unidades USB. Bloquear modificaciones de HOST. - Bloquear acceso de Autorun.inf.
  - Bloquea inicio de aplicaciones y extensiones.exe como Teamviewer, AnyDesk, VNC, OneDrive, Google Drive, etc.
- Politica de prueba-Control de Aplicaciones: Esta política fue creada con la finalidad de trabajar en entornos de pruebas o de laboratorio, para verificar como se comporta bloqueo de aplicaciones o dispositivos, antes de implementar sobre el entorno de producción.
- Application and Device Control policy-USB solo lectura: Política que reconoce dispositivos USB, pero solo en modo de lectura.
  - Bloquea acceso de Autorun.inf.
  - Bloquea escritura a dispositivos USB.
  - Bloquea el uso de Módems.
- DGA AULA- Política para Funcionarios Habilitados y Jefes: Esta política está creada para la utilización del grupo Equipos en cuarentena Habilitados DGICAULA.
  - Bloquea la ejecución de programas desde unidades externas.
  - Bloquear modificaciones de HOST.
  - Bloquear acceso de Autorun.inf.
  - Bloquea la ejecución de archivos .exe
  - Bloquea acceso a scripts (.bat, .reg, .vbs, .cmd)

- Bloquea herramienta de restablecimiento de contraseña.
- Bloquea módems.
- Bloquea inicio de aplicaciones como Teamviewer, AnyDesk, VNC, OneDrive, Google Drive, etc

- DGA AULA- Bloqueo Parcial Funcionarios:
  - Bloquea la ejecución de programas desde unidades externas.
  - Hacer que todas las unidades sean de solo lectura.
  - Bloquear escritura en unidades USB.
  - Bloquear modificaciones de HOST.
  - Bloquear acceso de Autorun.inf.
  - Bloquea la ejecución de archivos .exe
  - Bloquea acceso a scripts (.bat, .reg, .vbs, .cmd) -
  - Bloquea herramienta de restablecimiento de contraseña
  - Bloquea inicio de aplicaciones como Teamviewer, AnyDesk, VNC, OneDrive, GoolgeDrive, etc.

LiveUpdate:

Esta política está configurada para administrar y desplegar las actualizaciones de base de firmas de productos a los clientes que se conectan a la consola Symantec Endpoint Protection Manager. En el Ministerio de Hacienda todos los clientes utilizan el servidor de administración predeterminado para poder obtener las actualizaciones, los clientes no tienen un horario predeterminado para la búsqueda de actualizaciones, están configurados para realizarlo de forma continua. En caso de que el equipo cliente se encuentre inactivo el proceso de actualización se retrasa hasta que el mismo se encuentre activo y con acceso a las actualizaciones del Servidor de administración predeterminado.

- Los usuarios finales también tienen acceso a ejecutar de manera manual el proceso de actualización.

Política de Excepciones:

Esta excepción fue creada para el monitoreo de la aplicación FireFoxMH-22.0.3-win.exe para todos los clientes con S. E.P.

1- Esta excepción fue creada para el monitoreo de la aplicación FireFoxMH-22.0.3-win.exe para todos los clientes con S. E.P.
2- Esta fue creada para ser ignorada la aplicación FireFoxMH-22.0.3-win.exe en la carpeta C:\User\FRANCO_PRIETO\Downloads\Firefox11g.PNG.
3- Fue creada para ignorar la aplicación FireFoxMH-22.0.3-win.exe en la carpeta de C:\users\mdiequin\downloads\

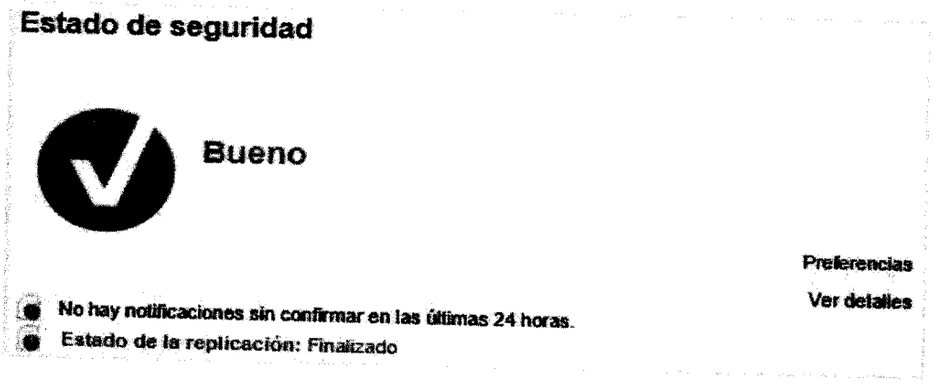
OLAM Carlos Herrera
Dpto. Licitaciones

4- Se creó para ser ignorada la aplicación FireFoxMH-22.0.3-win.exe dentro de la carpeta de C:\users\fraco_prieto\desktop\ff22\
5- Fue creada para ignorar el sitio 10.20.3.10 y verlo como Dominio Web de Confianza para todos los equipos clientes S.E.P.
6- fue creada para ignorar el sitio 10.2.8.11 y verlo como Dominio Web de Confianza para todos los equipos clientes S.E.P.
7- Se creó para ignorar la aplicación psi.exe desde la carpeta C:\program files (x86)\psi.exe para todos los equipos clientes S.E.P.
8- Se creó para ignorar la aplicación FM Screen Capture Códec (VFW) en la carpeta C:\windows\syswow64\fmcodec.dll para todos los clientes con S.E.P.
9- Fue creada para ignorar toda aplicación que este alojado en la carpeta c:\program files (x86)\common files\roxio shared\9.0\dragon\romlaucher.exe aplicado a todos los clientes S.E.P.
10- Esta excepción fue creada para ignorar la aplicación mysqld.exe desde la carpeta c:\program files\mysql server 5.5\bin\mysqld.exe aplicada a todos los clientes S.E.P.
11- Fue creada para ignorar www.cipfa.org como sitio de Dominio Web de Confianza aplicada a todos los clientes con S.E.P.
12- fue creada para ignorar la carpeta c:\discoverer\ para todo tipo de escaneo del AV aplicada a todos los clientes S.E.P.
13- Fue creada para ignorar fénix.hacienda.gov.py como sitio de Dominio Web de Confianza aplicada a todos los clientes con S.E.P.
14- Esta excepción fue creada para solo monitorear la aplicación FirefoxDiscoverer.exe*.exe para todos los clientes S.E.P.
15- Esta excepción fue creada para solo monitorear la aplicación SmdmFService para todos los clientes S.E.P.
16- Excepción para carpeta C:\siare\FirefoxMH41\FirefoxPortable.exe para todos los clientes S.E.P.
17- Fue creada para ignorar la aplicación DefaultTabUpdate en todos los equipos clientes con S.E.P.
18- Fue creada para ignorar FirefoxPortable.exe.

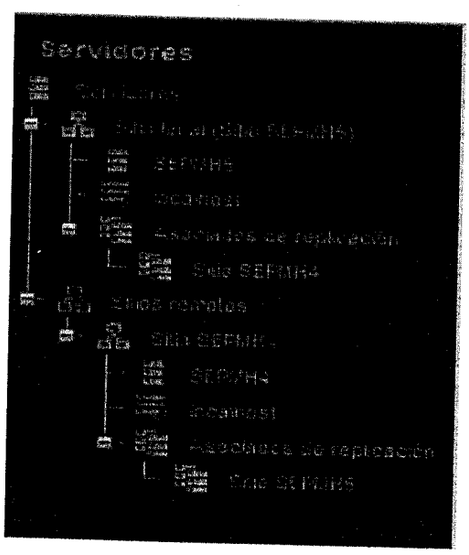
OLAM Carlos Herrera
Dpto. Licitaciones

2.3 Estado de replicación de servidores

El estado de replicación entre servidores se está realizando de forma normal, las mismas asumen entre si los cambios realizados entre SEPMH5 (primario) y SEPMH4 (contingencia)



La tarea esta programada para que los sitios se repliquen cada 4(cuatro) horas



Carlos Herrera
Dpto. Licitaciones

Propiedades del partner de replicación para Sitio SEPMH4

Partner

Nombre del partner: Sitio SEPMH4

Descripción:

Lista de servidores de administración de replicación:10.20.2.45
Ejemplo: <dirección IP>
<Host Name>

- [ ] Replicar registros desde el sitio local al sitio partner
- [ ] Replicar registros desde el sitio partner al sitio local
- [ ] Replicar paquetes de cliente entre el sitio local y este sitio partner

Programación

- ( ) Replicar automáticamente
  Permita que el servidor de administración decida cuándo debe ejecutarse la replicación.
- (•) Replicar según una programación
  Configure la programación de ejecuciones de replicación
  - (•) Cada hora ( ) Diaria ( ) Semanal
  - Cada: 4 Horas
  - Los: Lunes
  - Especifique el intervalo de tiempo durante el cual puede comenzar la replicación
  - Inicia a las: 00 : 00
  - Finaliza a las: 23 : 59

Carlos Herrera
Dpto. Licitaciones

2.4 Ultimas actualizaciones de los componentes de SEP

Se adjunta los recortes de todas las actualizaciones de los componentes

Ultimas definiciones de virus descargadas

Distribución de definiciones de virus

Actualizado desde 09/30/2018 11:45:00

Fecha de definición Revisión	Versión Informado a	Sistema operativo	Número de equipos	Porcent.	Distribución de definiciones de virus
10/01/2018 2	1/10/18 r2 10/01/2018 08:25:04	Windows	429	95.97%	
09/30/2018 22	30/9/18 r22 10/01/2018 05:54:46	Windows	12	2.68%	
09/30/2018 2	30/9/18 r2 09/30/2018 13:11:34	Windows	1	0.22%	
09/29/2018 1	29/9/18 r1 09/29/2018 15:08:20	Windows	1	0.22%	
09/28/2018 2	28/9/18 r2 09/28/2018 15:19:55	Windows	1	0.22%	
09/27/2018 20	27/9/18 r20 09/28/2018 07:47:21	Windows	1	0.22%	
08/16/2018 8	16/8/18 r8 08/16/2018 20:38:08	Windows	1	0.22%	
08/03/2018 2	3/8/18 r2 08/03/2018 13:08:52	Windows	1	0.22%	
Total			447	100%	

Lista del portal de AP versiones

Versión de patrón	Número de equipos	Porcent.
2018-08-13 rev. 002	**441**	**99.1%**
2017-07-17 rev. 033	**4**	**0.9%**
Total con la versión Lista del portal de AP	445	100%

Contenido SONAR versiones

Versión de patrón	Número de equipos	Porcent.
2018-09-24 rev. 007	**438**	**98.6%**
2018-09-14 rev. 001	**1**	**0.2%**
2018-09-04 rev. 001	**2**	**0.5%**
2018-01-17 rev. 005	**1**	**0.2%**
2017-10-11 rev. 003	**2**	**0.5%**
Total con la versión Contenido SONAR	444	100%

Descompresor versiones

Versión de patrón	Número de equipos	Porcent.
2.3.5.10	**444**	**99.6%**
2.3.3.2	**2**	**0.4%**
Total con la versión Descompresor	446	100%

Firma de prevención de intrusiones versiones

OLAM Carlos Herrera
Dpto. Licitaciones

Versión de patrón	Número de equipos	Porcent.
2018-09-28 rev. 063	**439**	**98.9%**
2018-09-27 rev. 061	**4**	**0.9%**
2018-08-16 rev. 061	**1**	**0.2%**
Total con la versión Firma de prevención de intrusiones	444	100%

Detección de endpoints y definiciones de respuesta versiones

Versión de patrón	Número de equipos	Porcent.
2018-08-16 rev. 017	**417**	**94.6%**
2017-04-13 rev. 014	**24**	**5.4%**
Total con la versión Detección de endpoints y definiciones de respuesta	441	100%

Firmas y atributos de archivo extendidos versiones

Versión de patrón	Número de equipos	Porcent.
2018-09-19 rev. 007	**375**	**84.3%**
2018-09-11 rev. 008	**52**	**11.7%**
2018-08-17 rev. 008	**14**	**3.1%**
2018-08-02 rev. 006	**1**	**0.2%**
2018-07-17 rev. 016	**1**	**0.2%**
2017-10-16 rev. 003	**2**	**0.4%**
Total con la versión Firmas y atributos de archivo extendidos	445	100%

Motor del borrador versiones

Versión de patrón	Número de equipos	Porcent.
117.3.1.6	**446**	**100%**
Total con la versión Motor del borrador	446	100%

Contenido de revocación versiones

Versión de patrón	Número de equipos	Porcent.
2018-10-01 rev. 004	**1**	**0.2%**
2018-09-30 rev. 037	**438**	**98.4%**
2018-09-30 rev. 033	**1**	**0.2%**
2018-09-30 rev. 020	**1**	**0.2%**
2018-09-30 rev. 007	**1**	**0.2%**
2018-09-28 rev. 006	**1**	**0.2%**
2017-10-15 rev. 022	**2**	**0.4%**
Total con la versión Contenido de revocación	445	100%

Definiciones de Power Eraser versiones

Carlos Herrera
Dpto. Licitaciones

Versión de patrón	Número de equipos	Porcent.
2016-11-21 rev. 023	**374**	**100%**
Total con la versión Definiciones de Power Eraser	374	100%

Biblioteca y configuración de transporte de red común versiones

Versión de patrón	Número de equipos	Porcent.
2018-07-05 rev. 033	**441**	**100%**
Total con la versión Biblioteca y configuración de transporte de red común	441	100%

Lista de aplicaciones permitidas de Symantec versiones

Versión de patrón	Número de equipos	Porcent.
2018-10-01 rev. 002	**440**	**98.9%**
2018-09-30 rev. 002	**2**	**0.4%**
2018-09-28 rev. 002	**1**	**0.2%**
2017-10-16 rev. 002	**2**	**0.4%**
Total con la versión Lista de aplicaciones permitidas de Symantec	445	100%

Definiciones de redirección de tráfico de WSS versiones

Versión de patrón	Número de equipos	Porcent.
2018-07-20 rev. 274	**406**	**100%**
Total con la versión Definiciones de redirección de tráfico de WSS	406	100%

Definiciones de virus versiones

Versión de patrón	Número de equipos	Porcent.
2018-10-01 rev. 002	**17**	**3.8%**
2018-09-30 rev. 022	**423**	**94.8%**
2018-09-30 rev. 002	**1**	**0.2%**
2018-09-29 rev. 001	**1**	**0.2%**
2018-09-28 rev. 002	**2**	**0.4%**
2018-09-27 rev. 020	**1**	**0.2%**
2018-08-16 rev. 008	**1**	**0.2%**
Total con la versión Definiciones de virus	446	100%

Carlos Herrera
Dpto. Licitaciones

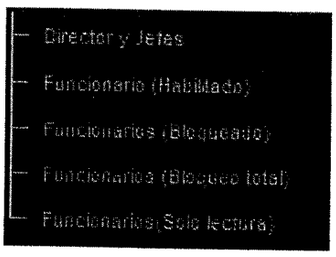
3 Implementación de ajustes de acuerdo recomendaciones

3.1 Actualización de políticas

Las políticas implementadas que se detallan en el ítem 2.2 no fueron modificados, ya se encuentran configurados y seteados de acuerdo a los pedidos sugeridos para cada dependencia.

3.2 Reglas

Para la aplicación de políticas existen 5 tipos de reglas aplicadas por grupo, de acuerdo al grado de permisos que se les otorga



Director y jefes: No tienen restricciones en cuanto a dispositivos USB, si algunas de aplicaciones como las de almacenamiento en la nube.

Funcionario Habilitado: Al igual que la anterior no tienen restricciones en cuanto a dispositivos USB, si algunas aplicaciones como las de almacenamiento en la nube.

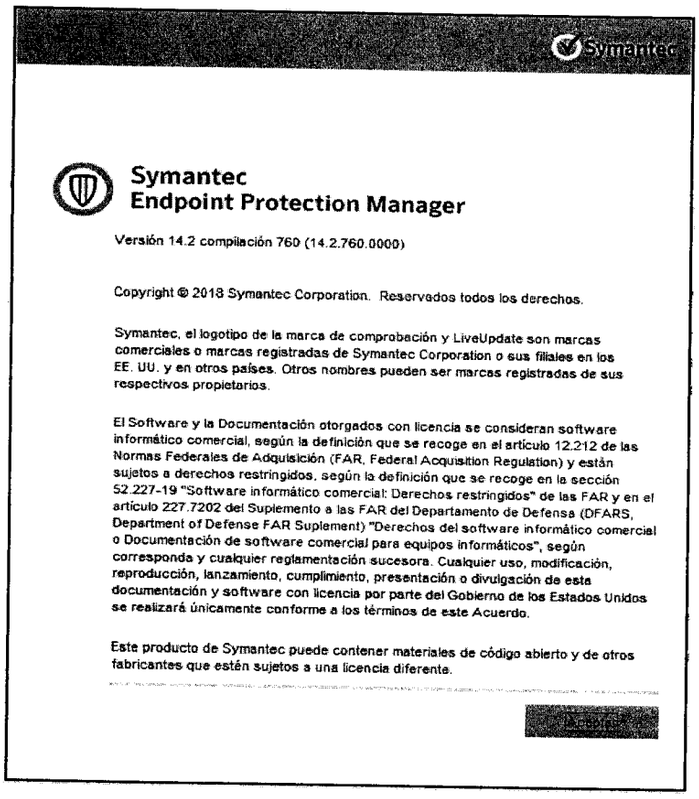
Funcionario Bloqueado: Tienen bloqueado el uso de modem, pendrives, lector de cd o dvd, y las aplicaciones de almacenamiento en la nube están bloqueadas.

Funcionario Bloqueo Total: Sin posibilidad de utilizar scanner, impresoras, ni dispositivos de almacenamiento USB, modems, dispositivos bluetooh etc, y tambien restricción de aplicaciones.

Funcionarios Solo lectura: Pueden utilizar dispositivos USB pero solo a modo de lectura, no se puede copiar archivos a la misma.

3.3 Alertas y últimas versiones disponibles

Ambos servidores SEPM fueron migrados de consola de la version 14.0.3676.1100 a la version de consola 14.2 compilacion 760 (14.2.760.0000), los equipos clientes estan siendo migrados de las versiones 12.1.5337.5000; 12.1.6306.6100; 12.1.70.61.6100; 14.0.2349.0100 y 14.0.3676.1100 a la version de cliente SEP 14.2.760.0000. Las versiones anteriores vienen siendo arrastradas de clientes que no se actualizaron o que se mantuvieron apagadas al momento de la migracion de version; con dichos clientes se trabajo en conjunto con DGIC a travez de listados de los equipos de las dependencias que estan afectadas.



Symantec

Symantec Endpoint Protection Manager

Versión 14.2 compilación 760 (14.2.760.0000)

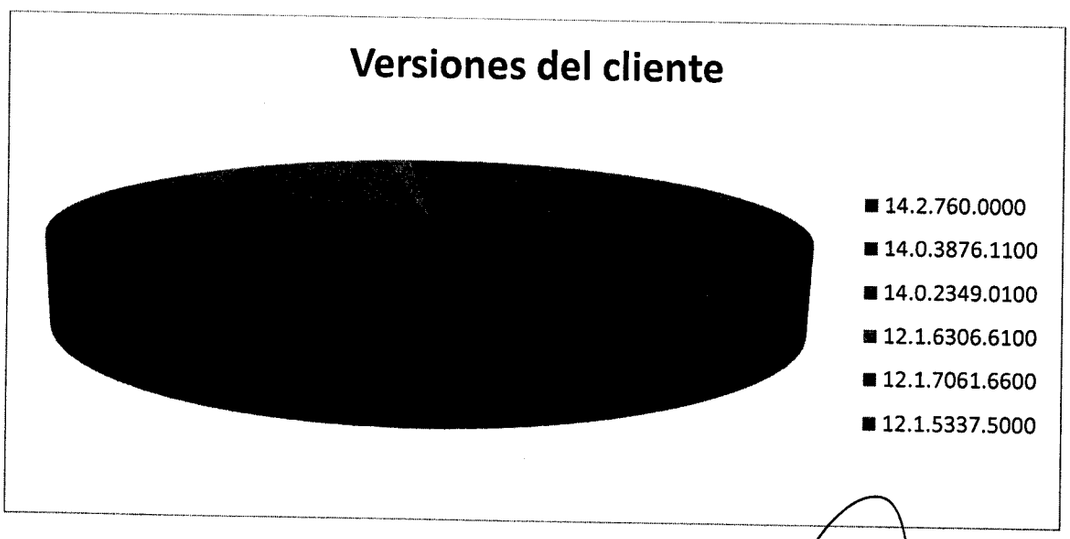
Copyright © 2018 Symantec Corporation. Reservados todos los derechos.

Symantec, el logotipo de la marca de comprobación y LiveUpdate son marcas comerciales o marcas registradas de Symantec Corporation o sus filiales en los EE. UU. y en otros países. Otros nombres pueden ser marcas registradas de sus respectivos propietarios.

El Software y la Documentación otorgados con licencia se consideran software informático comercial, según la definición que se recoge en el artículo 12.212 de las Normas Federales de Adquisición (FAR, Federal Acquisition Regulation) y están sujetos a derechos restringidos, según la definición que se recoge en la sección 52.227-19 "Software informático comercial: Derechos restringidos" de las FAR y en el artículo 227.7202 del Suplemento a las FAR del Departamento de Defensa (DFARS, Department of Defense FAR Suplement) "Derechos del software informático comercial o Documentación de software comercial para equipos informáticos", según corresponda y cualquier reglamentación sucesora. Cualquier uso, modificación, reproducción, lanzamiento, cumplimiento, presentación o divulgación de esta documentación y software con licencia por parte del Gobierno de los Estados Unidos se realizará únicamente conforme a los términos de este Acuerdo.

Este producto de Symantec puede contener materiales de código abierto y de otros fabricantes que estén sujetos a una licencia diferente.

El siguiente gráfico detalla las versiones de cliente de SEP informadas:



Carlos Herrera
Dpto. Licitaciones

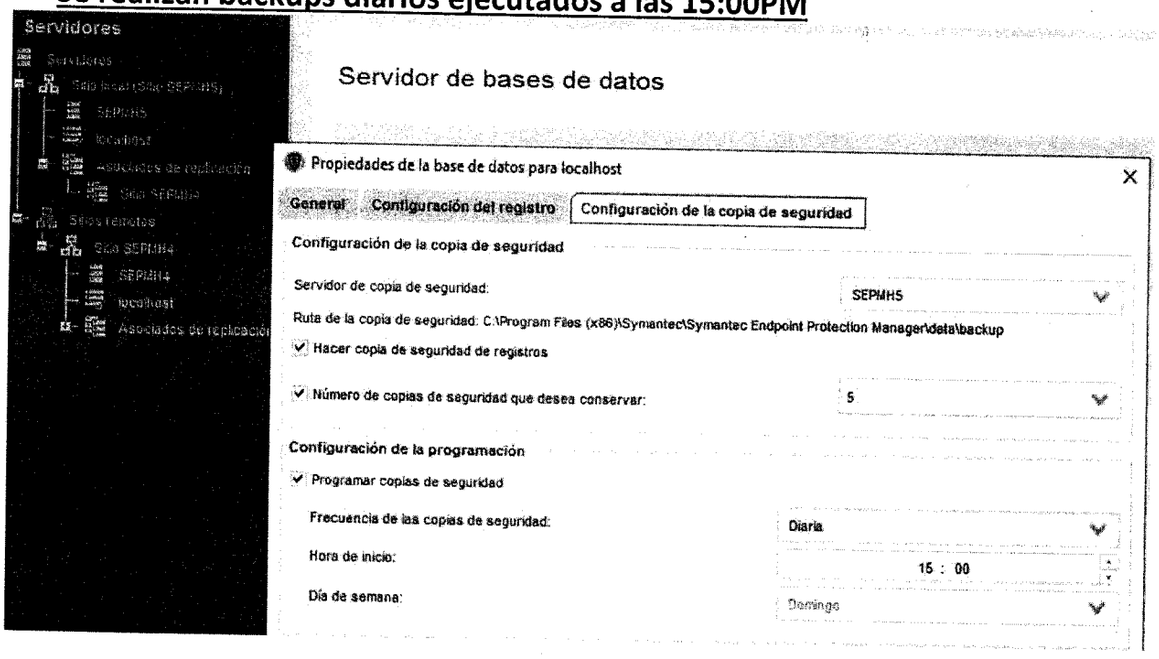
- Los equipos clientes están siendo migrados a la versión más reciente que es la 14.2.760.0000, las versiones anteriores según la tabla descriptiva corregirán las sugerencias de seguridad una vez que los clientes reciban la actualización a la nueva versión.
- Por lo general se aplica una tarea de distribución automática para la migración de versión, pero este solo aplica si el equipo se encuentra disponible en la red; no se ha instalado el 100% del parque actual de equipos porque siempre hay un margen de entre 100 a 150 equipos desconectados (sería un 20% del parque de equipos), estamos trabajando en conjunto con soporte DGIC para ubicar los equipos desconectados y aplicar las actualizaciones correspondientes.

Versión	Clientes	Plataforma del sistema operativo	Sugerencias de seguridad
12.1.5337.5000	2	Windows	Actualizar clientes a la versión 14.2.760.0000
12.1.6306.6100	6	Windows	Actualizar clientes a la versión 14.2.760.0000
12.1.7061.6600	4	Windows	Actualizar clientes a la versión 14.2.760.0000
14.0.2349.0100	27	Windows	Actualizar clientes a la versión 14.2.760.0000
14.0.3876.1100	33	Windows	Actualizar clientes a la versión 14.2.760.0000
14.2.760.0000	449	Windows	Ninguno

Carlos Herrera
Dpto. Licitaciones

3.4 Revisiones y pruebas de restauración de backup

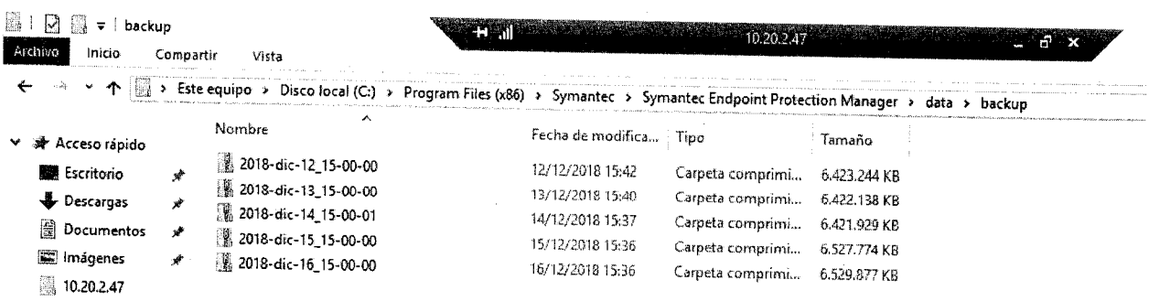
Se realizan backups diarios ejecutados a las 15:00PM



Ubicación de las copias de respaldo

Las mismas se alojan en el servidor de administración, guardando hasta cinco copias, al realizar una nueva sobre escribe la más antigua

La ubicación donde se aloja las copias de respaldo del servidor es en C:\Program Files(x86)\Symantec\SymantecEndpointProtectionManager\data\backup

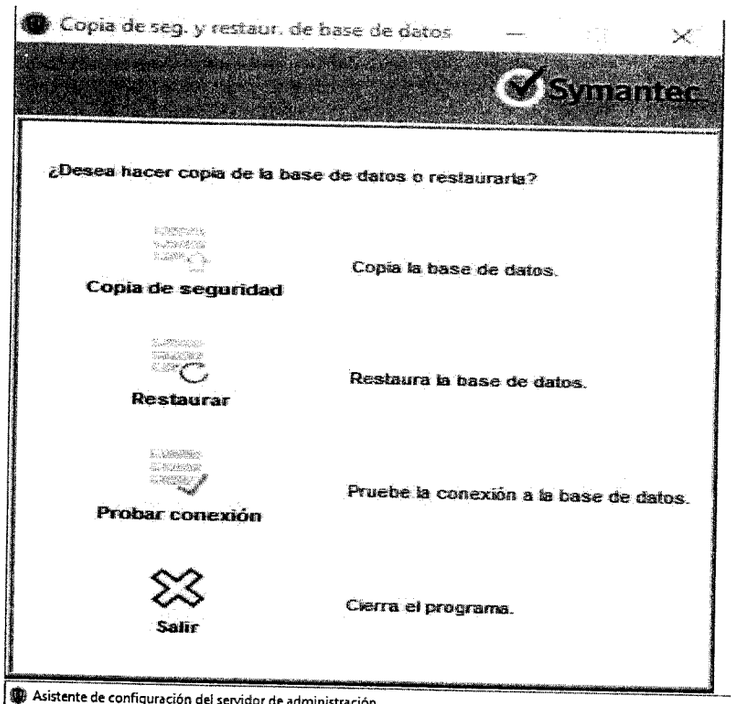


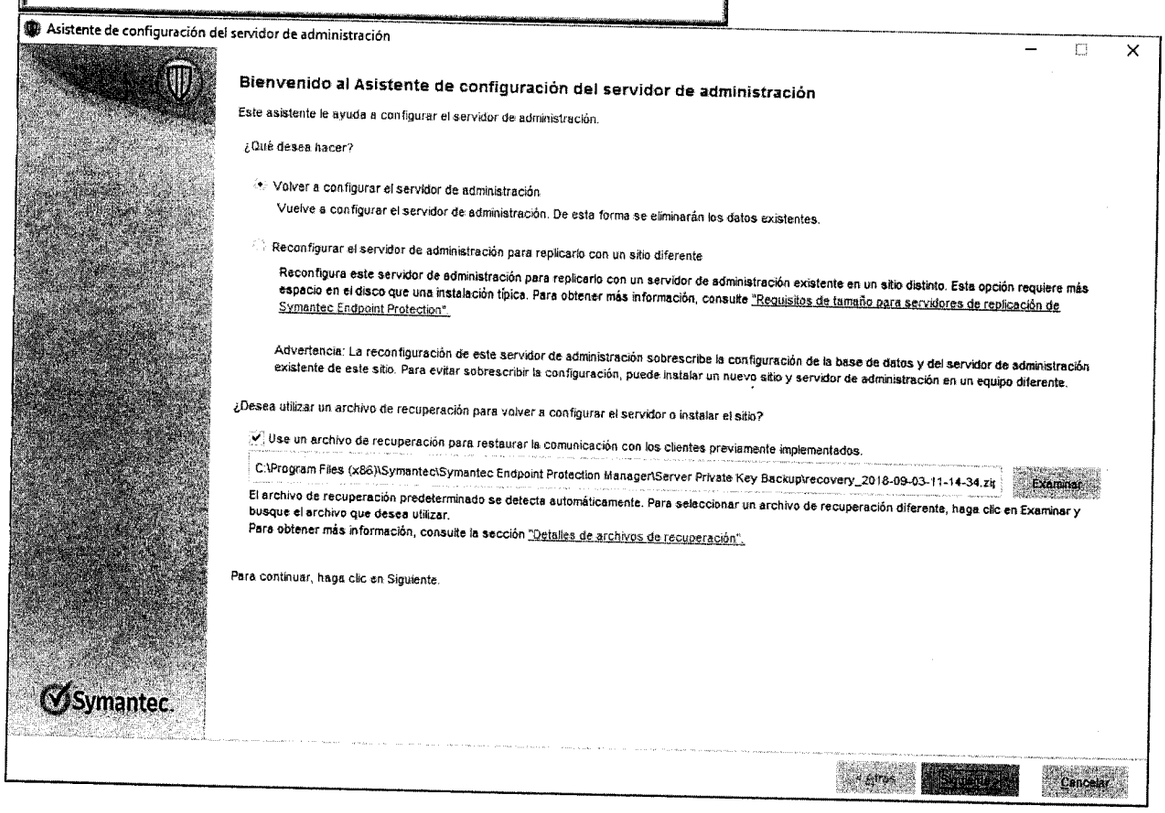
Las copias de seguriad tambien pueden generarse con la herramienta Copias de seguridad y restauracion de base de datos

Prueba de restauración de copias de seguridad

Se inicia el wizard de la herramienta backup and restore de SEPM, y se le indica el punto de restauracion que queremos iniciar, la misma no presenta inconvenientes, las copias de seguridad estan en funcionamiento.

Carlos Herrera
Dpto. Licitaciones


Copia de seg. y restaur. de base de datos
Symantec
¿Desea hacer copia de la base de datos o restaurarla?
Copia de seguridad
Copia la base de datos.
Restaurar
Restaura la base de datos.
Probar conexión
Pruebe la conexión a la base de datos.
Salir
Cierra el programa.


Asistente de configuración del servidor de administración
Bienvenido al Asistente de configuración del servidor de administración
Este asistente le ayuda a configurar el servidor de administración.
¿Qué desea hacer?
Volver a configurar el servidor de administración
Vuelve a configurar el servidor de administración. De esta forma se eliminarán los datos existentes.
Reconfigurar el servidor de administración para replicarlo con un sitio diferente
Reconfigura este servidor de administración para replicarlo con un servidor de administración existente en un sitio distinto. Esta opción requiere más espacio en el disco que una instalación típica. Para obtener más información, consulte "Requisitos de tamaño para servidores de replicación de Symantec Endpoint Protection".
Advertencia: La reconfiguración de este servidor de administración sobrescribe la configuración de la base de datos y del servidor de administración existente de este sitio. Para evitar sobrescribir la configuración, puede instalar un nuevo sitio y servidor de administración en un equipo diferente.
¿Desea utilizar un archivo de recuperación para volver a configurar el servidor o instalar el sitio?
Use un archivo de recuperación para restaurar la comunicación con los clientes previamente implementados.
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_2018-09-03-11-14-34.zip
Examinar...
El archivo de recuperación predeterminado se detecta automáticamente. Para seleccionar un archivo de recuperación diferente, haga clic en Examinar y busque el archivo que desea utilizar.
Para obtener más información, consulte la sección "Detalles de archivos de recuperación".
Para continuar, haga clic en Siguiente.
Symantec
Atrás
Siguiente >
Cancelar

4. Reporte de riesgos y ataques de red detectados y mitigados

Clientes verificados por tarea de análisis de virus

Los clientes de SEP pueden informarse como infectados cuando el proceso de reparación no se ejecuta correctamente o cuando aún existen acciones pendientes.

Una vez que un cliente se informa como infectado, el estado se borra automáticamente si no se requiere tomar medidas. El análisis de los clientes infectados informados debe ser un proceso administrativo regular.

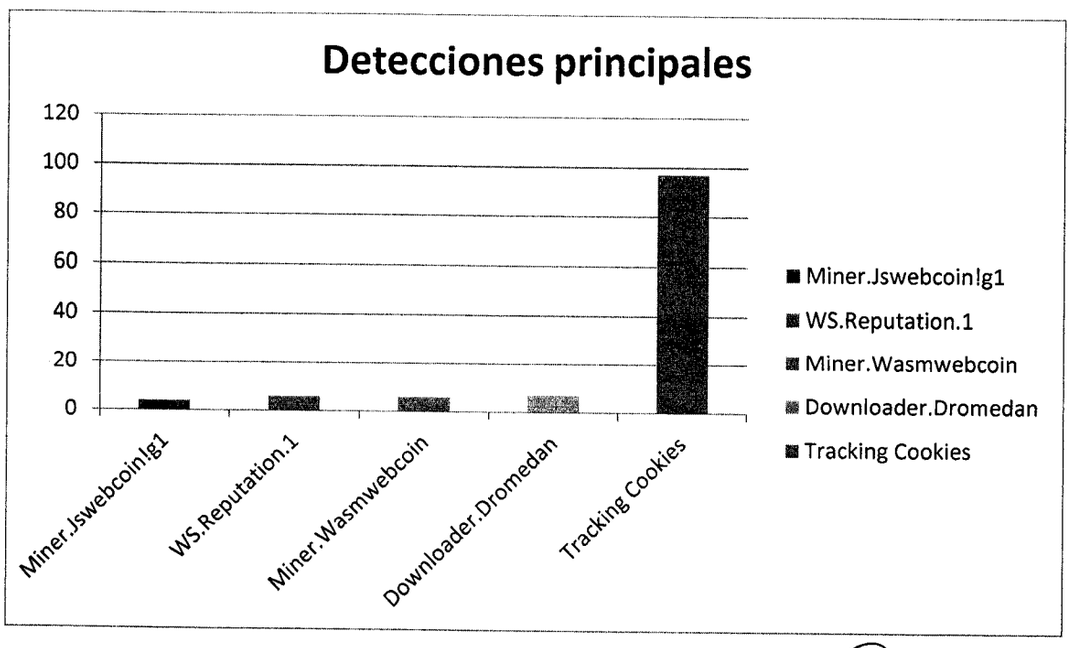
El siguiente gráfico detalla los cinco grupos que más clientes infectados informaron:

Dominio > Grupo	Clientes con estado Infectado
No se encontraron datos	

No se encuentran clientes en estado de infección.

Detecciones principales

Los datos en este gráfico han sido consolidados para que una infección se contabilice solo una vez por sistema y por tipo de análisis único, tipo de amenaza única y acción de reparación única.



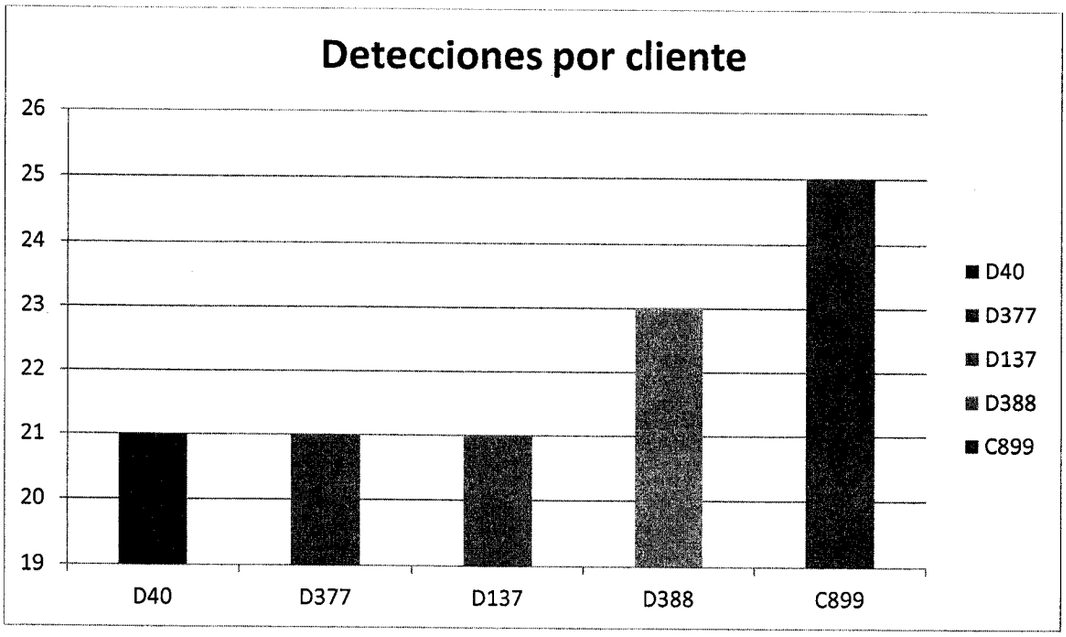
Nombre de la amenaza	Recuento
Tracking Cookies	97

Carlos Herrera
OLAM Dpto. Licitaciones

Nombre de la amenaza	Recuento
Downloader.Dromedan	7
Miner.Wasmwebcoin	6
WS.Reputation.1	6
Miner.Jswebcoin!g1	4

Detecciones por cliente

El siguiente gráfico detalla los clientes según la cantidad de detecciones:



Nombre del equipo	Detecciones
C899	25
D388	23
D137	21
D377	21
D40	21

Principales destinos bloqueados	Instancias	Porcentaje
F:/Autorun.inf	31	18.70%
E:/autorun.inf	29	17.50%
C:/Users/juan_aquino3/AppData/Local/Dropbox/Update/DropboxUpdate.exe	24	14.50%
C:\Program Files\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\ccSvcHst.exe	8	4.80%
C:/Users/javier_notario/AppData/Local/Dropbox/Update/DropboxUpdate.exe	4	2.40%

Carlos Herrera
Dpto. Licitaciones

Symantec. OLAM

Descripción General de Symantec Endpoint Protection Manager para Ministerio de Hacienda Setiembre 2018

C:/Users/user/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	4	2.40%
C:\Program Files\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\DoScan.exe	4	2.40%
D:/autorun.inf	3	1.80%
C:/Windows/SysWOW64/OneDriveSetup.exe	3	1.80%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.0.3876.1100.105\Bin\ccSvcHst.exe	3	1.80%
C:/Windows/SoftwareDistribution/Download/082f4cbb7bbe888323aec69272cd4bbf/inst/x86_microsoft-windows-w..for-management-core_31bf3856ad364e35_6.1.7601.23512_none_ccf44c0c24698897/winrm.cmd	3	1.80%
C:/Windows/SoftwareDistribution/Download/082f4cbb7bbe888323aec69272cd4bbf/inst/x86_microsoft-windows-w..for-management-core_31bf3856ad364e35_6.1.7601.23512_none_ccf44c0c24698897/winrm.vbs	3	1.80%
C:/Windows/SoftwareDistribution/Download/8dc4b2b42e69e8401e3a389242c17c2d/inst/x86_microsoft-windows-w..for-management-core_31bf3856ad364e35_6.1.7601.23512_none_ccf44c0c24698897/winrm.cmd	3	1.80%
C:/Windows/SoftwareDistribution/Download/8dc4b2b42e69e8401e3a389242c17c2d/inst/x86_microsoft-windows-w..for-management-core_31bf3856ad364e35_6.1.7601.23512_none_ccf44c0c24698897/winrm.vbs	3	1.80%
C:\Program Files\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\DWHWizrd.exe	2	1.20%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.0.3876.1100.105\Bin\DoScan.exe	2	1.20%
G:/autorun.inf	1	0.60%
I:/autorun.inf	1	0.60%
J:/autorun.inf	1	0.60%
c:/autoexec.bat	1	0.60%
C:/Users/DAU/apagar.bat	1	0.60%
e:/601505371015bca012/install.exe	1	0.60%
e:/2d7ef110759b17056a7512170177/install.exe	1	0.60%
C:/Program Files (x86)/Windows Media Player/wmplayer.exe	1	0.60%
C:/Users/cayetano_vera/AppData/Roaming/Spotify/Spotify.exe	1	0.60%
C:/Users/lizza_pampliega/AppData/Roaming/Spotify/Spotify.exe	1	0.60%
C:/Users/malcrod/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/mdelpan/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/mdersam/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/mfauval/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%

© 2018

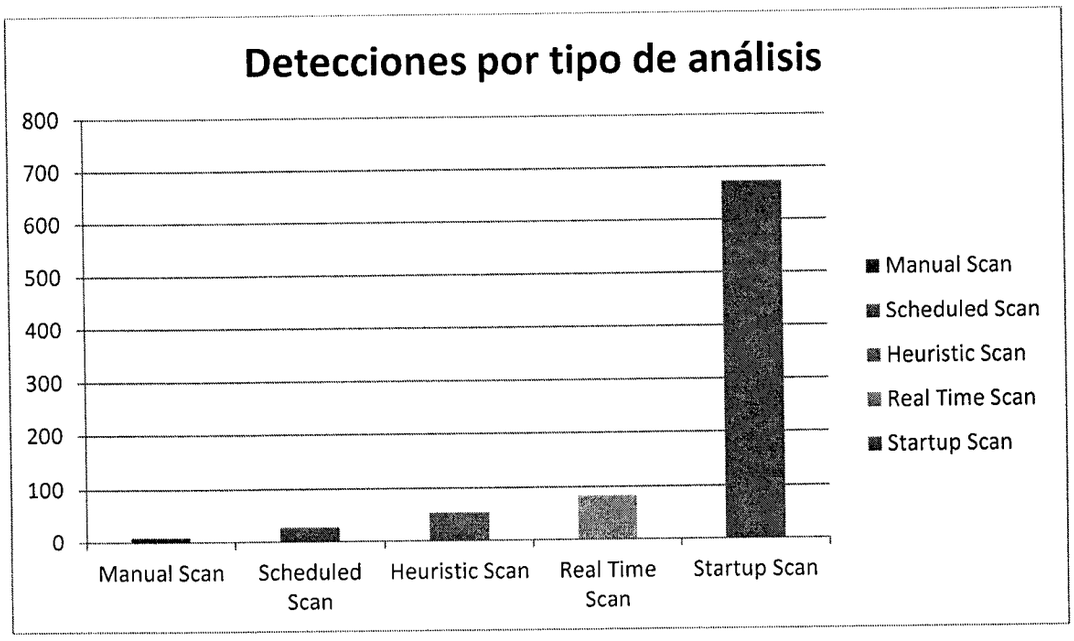
OLAM Carlos Herrera
Dpto. Licitaciones

C:/Users/mjuafer/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/tmareli/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/javier_notario/AppData/Roaming/Dropbox/bin/Dropbox.exe	1	0.60%
C:/Users/tjuceflo/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/diego_vera/AppData/Roaming/Spotify/SpotifyWebHelper.exe	1	0.60%
C:/Users/cayetano_vera/AppData/Roaming/Spotify/SpotifyWebHelper.exe	1	0.60%
C:/Users/martin_duarte/AppData/Roaming/Spotify/SpotifyWebHelper.exe	1	0.60%
C:/Users/Administrador/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/pablo_escobar/AppData/Local/Microsoft/OneDrive/OneDrive.exe	1	0.60%
C:/Users/lizza_pampliega/AppData/Roaming/Spotify/SpotifyWebHelper.exe	1	0.60%
C:/Users/malcrod/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/mdelpan/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/mdersam/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/menrpol/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/mfauval/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/mjuafer/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/tmareli/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:/Users/tjuceflo/AppData/Local/Microsoft/OneDrive/OneDriveStandaloneUpdater.exe	1	0.60%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\DoScan.exe	1	0.60%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.0.3876.1100.105\Bin\SmcGui.exe	1	0.60%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\ccSvcHst.exe	1	0.60%
C:\Program Files\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\Help\ClientHelp.chm	1	0.60%
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.760.0000.105\Bin\Help\ClientHelp.chm	1	0.60%
Total	166	100%

Carlos Herrera
Dpto. Licitaciones

Detecciones por tipo de análisis

En el siguiente gráfico, se detallan los 5 tipos de análisis principales que provocaron detecciones durante los últimos 30 días:

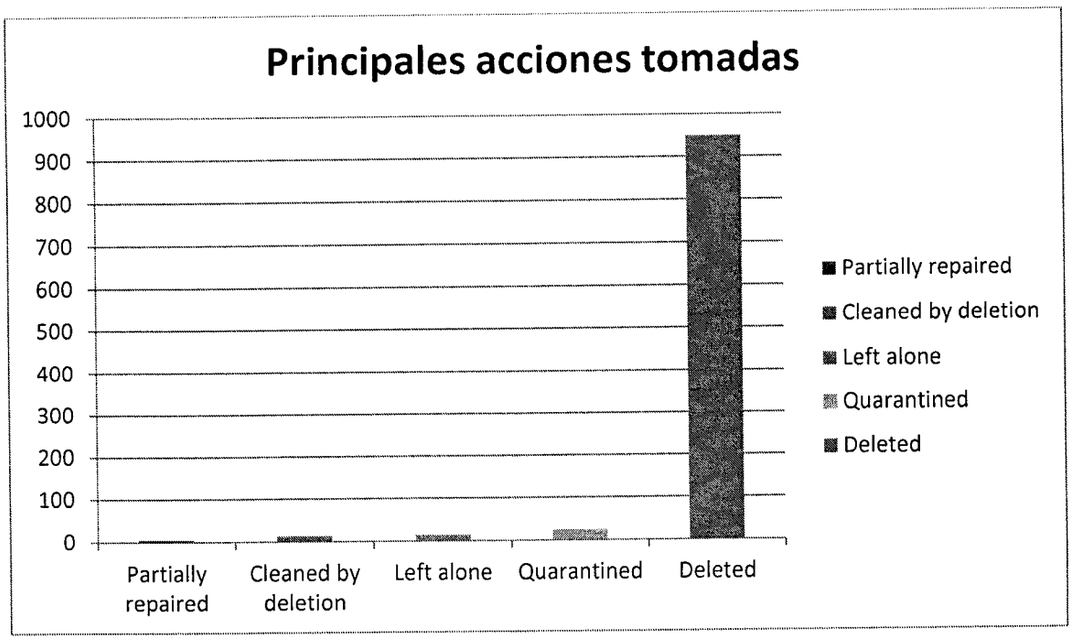


Origen	Recuento
Startup Scan	673
Real Time Scan	83
Heuristic Scan	53
Scheduled Scan	27
Manual Scan	9

Carlos Herrera
Dpto. Licitaciones

Principales acciones tomadas

En el siguiente gráfico, se detallan los 5 tipos de acciones principales realizadas contra amenazas detectadas durante los últimos 30 días:



Acción	Recuento
Deleted	746
Quarantined	19
Cleaned by deletion	15
Left alone	9
Cleaned	2

5 Recomendaciones

- Para un mejor panorama de distribución de la herramienta SEP, es necesario contar con un listado de todo el parque de equipos que componen la entidad, y a partir de ahí trabajar, verificar, y comparar con la consola de administración.
- También la depuración del DNS, para que los equipos clientes respondan de acuerdo con el nombre e IP que le corresponda.
- Dar siempre seguimiento a las implementaciones con la DGIC para estar al tanto de los cambios realizados.

Carlos Herrera
Dpto. Licitaciones

- En caso de no poder realizar la implementación de forma remota, ver la manera de realizarlo insitu con el cliente correspondiente.

- Dejar constancia de los pedidos de cambios realizados via mail, para mejor visualización de los trabajos realizados.

- Los usuarios administradores de la consola de Symantec, deben comunicar cualquier cambio realizado dentro de la consola (tareas, políticas, etc)

Carlos Harrera
Dpto. Licitaciones

43 cuatro mil y tres 29

Symantec

Luis Nuñez V.
Soporte Técnico
+595 974 733458
luis@olam.com.py
OLAM S.R.L.
Aviadores del Chaco 2462 e/ Santa Teresa y San Blas
Edificio Aura, Piso 7
Teléfono: **+595 21 601929**
Codigo Postal **1827**
http://www.olam.com
Asunción, Paraguay

OLAM
Microsoft GOLD CERTIFIED Partner

Reconocido por Microsoft en 2011 y 2013 como "Partner Country of the Year Award Winner"
Conozca más de OLAM y sus soluciones en nuestro sitio web y a través de las redes sociales

Carlos Herrera
OLAM Dpto. Licitaciones

Microsoft KASPERSKY eset SAMSUNG IBM UniFi hp SHARP GFi OLAM www.olam.com Symantec. Barracuda Veeam NetSupport ManageEngine Polycom COMODO Creating Trust Online redhat FORTINET

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Luis Nuñez	03:00	09:00	12:00	38857	03/Set/2018	Verificación de consola SEPM14. Se procede a verificar consola SEPM14, se ejecuta tarea de actualizacion de contenidos, se procede a actualizar las consolas de administracion del SEPMH4 y SEPMH5 de version 14.1 a la version 14.2.760.0000
Luis Nuñez	03:00	09:00	12:00	38861	05/Set/2018	Verificacion de consola SEPM14. Se procede a verificar consola SEPM14, se procede a crear los nuevos paquetes instaladores de SEP 14.2.760.0000 y es copiada a la gente de DGIC; se procede a crear en todos los grupos la tarea de upgrade de la herramienta para los equipos clientes los cualesmigraran de 14.1 a 14.2.760.0000.
Luis Nuñez	03:30	08:30	12:00	38863	07/Set/2018	Verificación de consola SEPM14. Se procede a verificar consola SEPM14, se procede a instalar por remoto SEp 14.2 en el grupo DGPNC en Directores y Jefes y Funcionarios Habilitados.
Luis Nuñez	03:30	08:30	12:00	38865	12/Set/2018	Verificacion de consola SEPM14. Se procede a verificar consola SEPM14, se procede a instalar los upgrade de version 14.2.760.0000 en los clientes SEP.
Luis Nuñez	03:00	09:00	12:00	38869	14/Set/2018	Verificacion de consola SEPM14. Se procede a verificar SEPM14; se crean seleccion de equipos en txt y se procede a actualizar cliente 14.0 a version 14.2.760.0000.
Luis Nuñez	03:00	09:00	12:00	38871	17/Set/2018	Verificacion de consola SEPM14. Se procede a verificar consola SEPM14, se ejecuta tarea de actualizacion de cliente SEP, de version 14.0 a version 14.3.760.0000.
Luis Nuñez	03:00	09:00	12:00	38875	21/Set/2018	Verificacion de consola SEPM14. Se procede a verificar consola SEPM14, las tareas de actualizacion automatica de version 14.2.760.0000 son seteadas para uqe los equipos clientes no reinicien de forma automatica.
Luis Nuñez	03:30	13:00	16:30	38876	24/Set/2018	Verificacion de consola SEPM14. Se procede a verificar consola SEPM14, se resetea contraseña administrador de Pedro Echeverria, se procede a cargar licencias nuevas y renovaciones en la consola de administracion, se crea lista detallada de equipos que aun poseen version SEP 12.
Luis Nuñez	03:30	08:30	12:00	38880	26/Set/2018	Verificacion de consola SEPM14.Se procede a verificar consola SEPM14, se trabaja sobre actualizacion de equipos D263;C946;D25;D129;D166 a version 14.2.760.0000; tambien se quitan print screen para preparacion de informe.Resultado:Se continuara con los trabajos.
Luis Nuñez	03:30	08:30	12:00	38877	28/Set/2018	Se procede a verificar consola SEPM14, se trabaja sobre actualizacion de equipos D263;C946;D25;D129;D166 a version 14.2.760.0000; tambien se quitan print screen para preparacion de informe.
Total	**32:30**	Horas Mes 1 Setiembre 2018				

Carlos Herrera
Dpto. Licitaciones

45 cuarenta y cinco

TETÃ VIRU MOHENDAPY
MOTENONDEHA
MINISTERIO DE HACIENDA

TETÃ REKUÁI
GOBIERNO NACIONAL

Paraguay de la gente

Subsecretaría de Estado de Administración Financiera
Dirección General de Informática y Comunicaciones

Asunción, 10 de enero de 2019.-

SSEAF/DGIC N° 024/19

Señora
Lic. MIRIAN ROLÓN, *Secretaria General*
Subsecretaría de Estado de Administración Financiera

Ref.: ***LCO 008/18 – Cto.051/18 – Servicios Profesionales para Mantenimiento y Configuración de Servidor Antivirus – ID 345.272***

Me es grato dirigirme a Usted, en relación a la Licitación de referencia, a los efectos de solicitar las Órdenes de Servicios y/o Compra correspondientes al Contrato mencionado y al mes de Septiembre/2018, con la Empresa adjudicada OLAM S.R.L.

La solicitud se realiza conforme a la **Licitación mencionada**, sujeta a los procedimientos y normativas pertinentes por parte de la Dirección Administrativa.

Se adjunta el Memo **DGIC/COTIC/DST N° 002/19** del Departamento de Soporte Técnico.

Sin otro particular, le saluda atentamente.

Lic. JUAN CARLOS FERREIRA MATTO
Encargado de Despacho Res. SSEAF N° 214/12
Dirección General de Informática y Comunicaciones

EXP. SIME Nº 1.726/2.019
Folio/s Nº (46) Cuarenta y seis.

Asunción, 10 de enero de 2.019

Se remite el presente expediente a la **Dirección Administrativa - CUOC**, a fin de proseguir con los trámites para la elaboración de la Orden de Servicio conforme a lo solicitado.

Lic. *Mirian Rolón*
Dep. S/ Res. SSEAF Nº 243/18
Dto. Administrativo - SSEAF

PRESIDENCIA DE LA REPUBLICA
Ministerio de Hacienda

Decreto Nro. 11766/08

PODER EJECUTIVO

Certificado de Disponibilidad Presupuestaria (CDP)

ANEXO B-02-04
Declaración Jurada

Nro. CDP 000000075/2019

Código C.C.: CO-12006-18-160201

Fecha Emisión 07/02/2019

Descripción CERTIFICACION DE SALDO DE CODIGO DE CONTRATACIÓN

Entidad 006 MINISTERIO DE HACIENDA

Tip	Pro	Sub Prg	Obj	Fue.	Fin.	Dpt.	UniR.	Descripción	1 Presupuesto Vigente	2 Plan Financiero Vigente	3 Compromisos	4 Modificaciones Presupuestarias	5 Certificacion Actual	6 Certificados Anteriores	7 = (5 + 6) Total Certificados	8= 2 - (3 + 4 + 7 Saldo Plan Financiero
2	001	03	00	260	10	1	99	SERVICIOS TECNICOS Y PROFESIONALES	8 832 410.000	8.832 410.000	13.000 000	0	140 000.000	143.000 000	283 000 000	8.536.410.000

Total PAC 140.000.000

Firma del Responsable de la Unidad de Presupuesto
Dionisio R. Sosa G.
Jefe
Departamento de Presupuesto

Firma del Responsable de la UAF
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros

Fermín Núñez
Dpto. Presu...

47 (cuarenta y siete)

MINISTERIO DE HACIENDA
S.S.E.A.F.
CRILIC04

Página: 1 / 1
Fecha: 08/02/2019
Hora: 09:25:25

Certificado de Disponibilidad Presupuestaria (CDP)
ANEXO B-02-04
Declaración Jurada
Decreto Nro. 8885/07

Nro. CDP 000000079/2019

Fecha Emisión 08/02/2019

Descripción CERTIFICACION DEL PAC PLURIANUAL Nro.: 345272 - CC: CO-12006-18-160201 Contratacion de Servicios profesionales para el Mantenimiento y Configuración del Servidor Antivirus de la DGIC del MH

Modalidad Concurso de Ofertas

Entidad 006 MINISTERIO DE HACIENDA

Nro P.A.C 07133509

AÑO 2019

PLURIANUAL

Tip	Prc.	Sub Prg	Obj	Fue.	Fin.	Dpt.	UnR.	Descripción	1 Presupuesto Vigente	2 Plan Financiero Vigente	3 Compromisos	4 Modificaciones Presupuestarios	5 Certificación Actual	6 Certificados Anteriores	7 = (5 + 6) Total Certificados	8= 2 - (3 + 4 + 7 Saldo Plan Financiero
2	001	03	00	269	10		99	4 SERVICIOS TÉCNICOS Y PROFESIONALES	8,832,410,000	8,832,410,000	13,000,000	0	44,000,000	283,000,000	327,000,000	8,492,410,000

Total PAC 44,000,000

Firma del Responsable de la Unidad de Presupuesto
Darnelio R. Sosa G.
Jefe
Departamento de Presupuesto

Firma del Responsable de la UAF
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros

Fermín Núñez
Dpto. P...

(ocho millones)

- Reporte de riesgos y ataques de red detectados y mitigados.
- Recomendaciones finales.

13. MODALIDAD DE PAGO

El pago se realizará en base a los productos esperados e informes de trabajos realizados los cuales serán entregados a los treinta (30) días de recepcionada las Órdenes de Servicio por parte del proveedor conforme al siguiente cuadro:

% contrato	Fecha	Documento Requerido
5%	A los treinta (30) días de la recepción de Orden de Servicio 01/12 por parte del Proveedor	Informe Inicial: Aprobado. Este documento debe incluir todos los informes, y documentaciones solicitadas en el Plan de Entregas.
5%	A los treinta (30) días de la recepción de Orden de Servicio 02/12 por parte del Proveedor	2°. informe mensual: Aprobado
5%	A los treinta (30) días de la recepción de Orden de Servicio 03/12 por parte del Proveedor	3°. informe mensual: Aprobado
5%	A los treinta (30) días de la recepción de Orden de Servicio 04/12 por parte del Proveedor	4°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 05/12 por parte del Proveedor	5°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 06/12 por parte del Proveedor	6°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 07/12 por parte del Proveedor	7°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 08/12 por parte del Proveedor	8°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 09/12 por parte del Proveedor	9°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 10/12 por parte del Proveedor	10°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 11/12 por parte del Proveedor	11°. informe mensual: Aprobado
10%	A los treinta (30) días de la recepción de Orden de Servicio 12/12 por parte del Proveedor	Informe Final: Aprobado. Este documento debe incluir todos los informes, y documentaciones solicitadas en el Plan de Entregas

OBS:

- **La DGIC solicitará la emisión de las órdenes de servicios desde la fecha del contrato de forma mensual.**
- **Todos los pagos se realizarán a los 60 días de presentado la solicitud de pago.**