Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires
Fiscalía General
Secretaría de Coordinación Administrativa
Oficina de Infraestructura
Departamento TI y Comunicaciones

ANEXO II a la Disposición UOA N° 42/17 – Pliego de Especificaciones Técnicas

RENGLON Nº 1: Adquisición y puesta en funcionamiento de una Solución de seguridad para las estaciones de trabajo y servidores del MPF.

Se requiere el suministro y puesta en funcionamiento de una solución de seguridad para estaciones de trabajo, servidores físicos y Virtuales con como mínimo las siguientes funcionalidades:

1. Solución de seguridad de Endpoint para estaciones de trabajo y servidores físicos con las siguientes características:

A	Aspectos Generales de la solución de Endpoint
A.1	Debe por lo menos tener las siguiente capacidades: Antimalware; Host IPS; Control de Navegación en el host ; Full disk Encryption y Firewall.
A.2	Estas capacidades detalladas en el punto A.1 deben ser parte de un único agente con módulos configurables.
A.3	Se debe poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.
A.4	La solución debe poder desplegar una aplicación cliente *standalone* que pueda gestionar cambios localmente en caso de que se necesite.
A.5	Se debe poder restringir completamente o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.
A.6	La desinstalación de la aplicación debe poder ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.
B	**Antimalware**
B.1	La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente.
B.2	Se debe poder configurar acciones sobre infecciones identificadas: Las acciones mínimas a incluir son: Denegar acceso ; Limpiar ; Eliminar ; Ninguna
B.3	La solución debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.
B.4	Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.
B.5	La solución debe poder habilitar la opción de escaneo de click-derecho sobre carpetas específicas.
B.6	La solución debe soportar archivos DAT V2 y V3 de detección de amenazas.
B.7	Debe contar con mecanismos de protección de exploits Generic Buffer Overflow Overflow Protection (GBOP) o integración con Microsoft DEP (Data Execution Prevention).
B.8	La solución debe contar con características de protección Kevlar para navegadores web (Active X).
B.9	La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de IE, sean JavaScript o VBScript.
B.10	La solución debe poder configurar mediante reglas o políticas de protección: • Entradas y llaves de registro de Windows. • Prevención de creación de ejecutables portables (.INI, .PIF).

	• Creación de archivos autorun. • Prevención de uso de archivos TFTP (Trivial File Transfer Protocol). • Contra lectura de archivos en cache de IE. • Creación y modificación remota de archivos o carpetas. • Acceso remoto de archivos o carpetas. • .EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT. • Modificación de procesos core de Windows. • Modificación de configuraciones de exploradores y navegadores web.
B.11	La solución debe soportar al menos los siguientes sistemas operativos de servidores: • Windows Server 2012, 2012 R2, and 2012 R2 Update 1: Essentials, Standard, Datacenter (incluyendo Server Core mode). • Windows Storage Server 2012 and 2012 R2 • Windows Server 2008 and 2008 R2: Standard, Datacenter, Enterprise, Web (incluyendo Server Core mode) • Windows Storage Server 2008 and 2008 R2
B.12	La solución debe soportar al menos los siguientes sistemas operativos de clientes: • Windows 10 Anniversary Update • Windows 10 November Update • Windows 10 • Windows 8.1 Update 1 • Windows 7 • Windows Vista • MAC Sierra 10.12 • MAC El Capitan 10.11
B.13	La solución de antivirus debe ser además compatible con sistemas Linux CentOS, Red Hat, SuSe y Ubuntu. Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado. No se aceptará tener que definir políticas diferentes para diferentes sistemas operativos.
C	**Antimalware para Email Server**
C.1	Debe contar con una solución que permita proteger específicamente al email Server.
C.2	Debe detectar URLs en correos electrónicos y bloquear de acuerdo a su reputación.
C.3	Debe permitir realizar exclusiones de escaneo en subfolders de la casilla de correo.
C.4	La solución debe permitir la definición de reglas de DLP.
C.5	Debe ser administrado por la misma consola que la solución de Antimalware.
C.6	Debe tener que poder escanear archivos comprimidos en 7-Zip.
C.7	Debe contar con la posibilidad de remover DATs viejos de los equipos administrados
C.8	Debe contar con funcionalidades de filtrado de contenido y soportar para esta funcionalidad expresiones regulares.
C.9	Debe permitir la posibilidad de realizar filtrado de archivos basado en nombre, tipo y tamaño.
C.10	Debe tener que contar con la posibilidad de realizar filtrado de correos basado en la reputación del sender.
C.11	Debe contar con la opción de escanear archivos basados en extensiones MIME.
C.12	La solución debe tener una administración de cuarentena ya sea base de datos local o un administrador de cuarentenas del fabricante.
C.13	Debe contar con funcionalidades que permitan la detección de ataques de denegación de servicio.
C.14	Debe contar con actualizaciones periódicas y programables.
C.15	Debe soportar email versión Exchange 2010 o superior y Sistema Operativo Windows 2012 r2 o superior.
D	**Firewall**
D.1	El módulo debe permitir/bloquear tráfico de red para todo tipo de protocolos.
D.2	Debe habilitar/deshabilitar protección IP Spoof
D.3	Debe habilitar/deshabilitar alertas de intrusión de Firewall.
D.4	Debe poder agregar dominios específicos para bloqueo DNS.
D.5	La solución debe poder recopilar log en eventos lanzados directamente sobre el

	cliente y reportar incidentes en la consola de administración central.
D.6	Cada una de las reglas debe ser aplicable tanto para tráfico entrante como para tráfico saliente del cliente.
D.7	Las reglas de tráfico deben ser soportadas para protocolos IPv4 e IPv6.
D.8	La solución debe aplicar reglas de tráfico para conexiones: Cableadas; Inalámbricas y Virtuales.
D.9	Las reglas de tráfico deben poder extenderse a ejecutables por medio de la especificación de ruta (se pueden utilizar wildcards).
D.10	El módulo debe poder incluir reglas predefinidas en base a los protocolos y puertos conocidos (well-known)
D.11	Se debe poder administrar redes y ejecutables de confianza desde la interfaz de usuario de los endpoints.
D.12	La herramienta debe contar con un mecanismo de conocimiento global de amenazas que permita configurar bloqueo de conexiones de alto riesgo en base a reputación.
E	**Control de Navegación**
E.1	La solución debe poder bloquear de forma automática sitios con clasificación de riesgo alto que puedan afectar los equipos y/o la red.
E.2	La solución debe tener la capacidad de bloquear y/o dejar al usuario decidir qué acción tomar en caso que el sitio que se esté visitando por alguna razón no cuente con una clasificación en ese momento.
E.3	La solución debe contar con un elemento visual que permita identificar el riesgo del sitio visitado en los navegadores soportados.
E.4	La solución incluso debe tener la capacidad de definir reglas de filtrado de URL por categoría.
E.5	La solución debe tener la capacidad de evitar el acceso a sitios de phishing.
E.6	La solución debe poder evitar descargar malware, ayudando así a tener que la protección sea proactiva.
E.7	La solución debe de contar con al menos 80 categorías de sitios web.
E.8	La solución debe poder especificar que navegadores sean los únicos autorizados para navegar a internet.
E.9	La solución debe tener la capacidad de definir rangos de IP privadas (intranet) que no sean analizadas por la herramienta para bloqueo de sitios web.
E.10	La solución debe tener la capacidad de forzar búsquedas seguras con los buscadores al menos cuatro de los motores de búsqueda más usados (Google, MSN, Yahoo, Terra, UOL, Ask).
E.11	La solución debe poder bloquear iFrames de HTML o advertir de sitios que contengan.
E.12	La solución debe tener categorías sincronizadas con una base de datos de reputación global de amenazas.
E.13	La clasificación debe ser en tiempo real y contra una base de datos de reputación que al menos correlacione archivos, URL´s, y correos electrónicos todo esto en la nube.
E.14	La solución debe tener la capacidad de personalizar los mensajes que le aparezcan al usuario cuando una política sea violada.
E.15	La solución debe tener la capacidad de definir un logotipo para mostrarlo en los mensajes de violación a las políticas.
E.16	Se deben poder ver reportes de amenazas web detectadas y políticas violadas.
E.17	La solución debe captar logs o registros para eventuales temas de compliance y troubleshooting.
E.18	La solución debe estar en la capacidad de identificar cuando el cliente se encuentra bajo la protección de una solución de proxy y desactivarse en la presencia de este.

F	Control de Dispositivos
F.1	La solución debe tener la capacidad de inspeccionar documentos en tiempo real en búsqueda de información confidencial y tomar acciones. Dentro de las condiciones de análisis deberá incluir (pero no limitarse) a aplicación que está escribiendo el archivo, tipos de archivos.
F.2	La solución debe tener la habilidad de crear reglas de excepción basada en una ventana de tiempo.
F.3	La solución debe poder alertar al usuario de sus acciones mediante mensajes personalizados.
F.4	La solución debe tener la habilidad de crear patrones personalizados de expresiones regulares (RegEx) para ser usados en reglas de protección de medios removibles.
F.5	La solución debe poder asignar reglas de protección basado en usuarios o grupos del Directorio Activo.
F.6	La solución debe poder monitorear la actividad del usuario en modo silencioso (sin alertar al usuario).
F.7	La solución debe soportar contenido pre-definido regulatorio como SOX, PCI e HIPAA.
F.8	La solución debe poder agregar a listas blancas y negras dispositivos por vendedor o ID del mismo.
F.9	La solución debe poder soportar por defecto por lo menos (pero no limitado a) los siguientes dispositivos: bluetoooth, CD/DVD, Discos Floppy, de Imagen, Infrarojos (IrDA), Memorias, Modems, Fax, Palms, adaptadores PCMCIA, Pocket PC, Puertos (COM y LPT), Manejadores de Cintas, Secure Digital Host Controllers, de transferencia de cables, USB, Windows Portables, equipos de comunicación inalámbrica, biométricos, Decoders, GPS, IEEE 1284.4 y 1394, Infiniband, teclados, Media Center Extender, transformadores de multimedia, Memory Technology Drivers (PCMCIA/Flash), mouses y apuntadores, Microsoft Common Controller for Windows Class, Multifuncionales, equipos multimedia, adaptadores multi puerto serial, adaptadores de red, clientes de red, servicios de red, transporte de red, drivers no plug-n-play, NT APM, Aceleradores PCI SSL, impresoras, controladores SCSI y RAID, dispositivos de seguridad, lectores para Smart Cards y dispositivos de audio.
F.10	La solución debe poder bloquear dispositivos "Plug-and-Play".
F.11	La solución debe permitir el uso de dispositivos de almacenamiento removibles como "Solo Lectura".
F.12	La solución debe permitir el uso de dispositivos de almacenamiento removible como "Sólo Lectura" a menos de que estén cifrados.
F.13	La solución debe poder auditar la conectividad de los dispositivos.
F.14	La solución debe integrarse de forma nativa con soluciones de cifrado de archivos y DLP (Toma de acciones, política única, agente único).
F.15	Las políticas de control deben restringir si aplican cuando la herramienta se encuentra dentro o fuera de un ambiente seguro (modo online/offline).
F.16	La solución debe poder permitir la importación masiva de definiciones de dispositivo (archivo CSV o similar).
F.17	La solución debe contar con habilidades de auto protección que evite la manipulación por terceros no autorizados.
F.18	La solución debe tener reglas de control específicas de fábrica para los siguientes dispositivos (pero no limitado a) : Discos Duros Fijos, Dispositivos Plug-n-Play, Almacenamiento Extraíble, Dispositivos TrueCrypt, Acceso a archivos desde medios removibles y Dispositivos en Citrix XenApp.
F.19	Debe permitir agregar varios usuarios de tipo administrador global, administrador de grupo, revisor global, revisor del sitio. Los revisores solo tienen acceso lectura.
F.20	Debe integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de la red con sus respectivos permisos.

2. Solución de Antivirus y seguridad para servidores Virtuales con las siguientes características mínimas:

H	Seguridad para Servidores Virtuales
H.1	Se requiere una solución de Antivirus especialmente optimizada para trabajar en

	entornos de virtualización que elimine la necesidad de instalar agentes de antivirus en cada máquina guest, donde esta funcionalidad este soportada, o tenga un agente especializado para esta función (debe ser diferente al agente tradicional de AV).
H.2	Debe controlar que las máquinas que están bajo un mismo hipervisor, no ejecute los scans en forma simultánea, lo que podría afectar la performance del sistema.
H.3	Debe soportar escaneos al momento que un archivo es accedido y por demanda.
H.4	Debe soportar escaneos de todos los archivos en una máquina virtual permitiendo además programar la frecuencia de los mismos.
H.5	Debe soportar al menos las siguientes plataformas de virtualización: Microsoft Server 2012 Hyper-V o posterior Vmware ESXi 5.x o posterior Citrix XenServer 6 o superior
H.6	Debe soportar los siguientes sistemas operativos en máquinas guests: Windows Server 2016 (64-bit) Windows 2012 R2 (64-bit) Windows 2012 Windows 2008 R2 (64-bit) Windows 2008 (32-bit)
H.7	Debe descubrir e importar para inventario las instancias de máquinas virtuales tanto las que están corriendo como las que se encuentran apagadas.
H.8	La solución debe contar con un cache que permita optimizar los recursos evitando escanear archivos que ya se hayan analizado anteriormente y no hayan sufrido cambios. Este caché debe ser tanto local en cada máquina virtual como central en cada escáner.
H.9	El tamaño del cache debe ser configurable.
H.10	Debe permitir configurar la cantidad de escaneos simultáneos a realizar en cada escáner.
H.11	Debe poder configurarse el tipo de archivos a escanear.
H.12	Debe mantener una cuarentena local en cada server en caso de detección de una amenaza. Debe permitir además configurar si se quiere mantener el archivo o eliminarlo.
H.13	Debe ser capaz de escanear unidades de red.
H.14	Debe soportar vMotion
I	**Arquitectura para el entorno virtual.**
I.1	La solución debe estar gestionada en forma centralizada a través de la misma consola que pueda ser utilizada para gestionar agentes de Antivirus tradicional.
I.2	Debe contar con escáners que ejecuten análisis de antivirus fuera de línea.
I.3	Debe además contar con un componente que gestione y asigne máquinas virtuales en forma automática a estos escáners en base a la carga, a preconfiguraciones o a rangos de IP.
I.4	Este componente debe soportar la implementación en Alta Disponibilidad.
I.5	Debe contar con escáners en Alta Disponibilidad con posibilidad de instalarlo dentro o fuera del cluster.
I.6	Debe contar con una opción de despliegue que no requiera agente en la máquina virtual utilizando las capacidades del ambiente. Indicar en que plataformas está

	soportado y de que manera se integra.
I.7	Debe contar con la capacidad de crear reglas de firewall de manera de aislar ciertos recursos del Data Center Virtual y protegerlos de amenazas provenientes de otros recursos dentro de la misma infraestructura.
I.8	Debe no ser necesario requerir reiniciar el hipervisor durante ningún paso del proceso de instalación de la solución.
I.9	Debe soportar el autoescalamiento de las máquinas virtuales de análisis (motores de detección externos), es decir que se debe poder programar la cantidad de estos equipos necesarios para un número máximo de clientes, en el caso en que dinámicamente este valor se incremente, estos dispositivos se deben aprovisionar de forma automática en el hipervisor para poder soportar la nueva carga.
J	**Integración del entorno virtual**
J.1	Debe conectarse a una base de reputación global de amenazas donde obtenga información de nuevas vulnerabilidades y nuevos contenidos maliciosos y provea inteligencia para la detección eficiente de ataques.
J.2	Debe soportar la integración nativa con un sistema de reputación local de inteligencia contra amenazas a través de un protocolo de comunicación en tiempo real diseñado para este fin, sin necesidad de un proceso de actualización de firmas o "llamado/despertar" de agentes o motores de análisis
J.3	Debe soportar la integración nativa con sistemas de detección avanzada de amenazas (sandbox), el resultado de este análisis (cambio de reputación local) debe ser compartido con toda la infraestructura en tiempo real, mediante un protocolo de comunicación diseñado para este fin, sin necesidad de un proceso de actualización de firmas o "llamado/despertar" de agentes o motores de análisis
K	**Gestión del entorno virtual**
K.1	La consola de gestión debe permitir designar las máquinas virtuales para cada escáner.
K.2	Debe permitir configurar la programación de los escaneos.
K.3	Debe contar con políticas de exclusión de escaneo de ciertos archivos y programas.
K.4	La solución debe descargar actualizaciones y motores de análisis periódicamente de manera automática y aplicarlas a los demás componentes de la solución.
K.5	Se deben poder definir hasta una política por máquina virtual.
K.6	La política debe ser única, independientemente del modo de despliegue (sin agente o con agente optimizado)

3. Sistema colaborativo de amenazas de día 0 para prevenir ataques avanzados en todas sus terminales, que cumplan con los siguientes puntos como mínimo.

L	Aspectos Generales del sistema colaborativo de amenazas de Día 0
L.1	La solución deberá permitir generar una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido virtual o en los equipos de usuario final para que puedan intercambiar información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito.
L.2	La solución deberá permitir a los administradores de seguridad ejecutar acciones de: bloqueo, limpiado, envío para análisis avanzado (sandbox), solicitud justificación de la ejecución al usuario.
L.3	La solución deberá proteger proactivamente al usuario de la ejecución de archivos ejecutables, que pudiesen representar un riesgo, basado en un sistema de reputación local (organizacional), sin necesidad de firmas o actualizaciones de fábrica.

L.4	La solución deberá permitir reputar archivos localmente (de forma manual o a través de reglas de comportamiento) y mediante distintas fuentes de reputación dentro de la infraestructura de seguridad como: Sandbox y Proxys Web)
L.5	La solución deberá poder integrarse a fuentes de reputación de software públicas. Ej Virustotal
L.6	La solución debe hacer posible que los administradores personalicen fácilmente la información integral sobre amenazas procedente de fuentes de datos globales (VirusTotal y Redes globales de reputación de la marca) y de fuentes de terceros (IOC), basado en su criterio en seguridad informática.
L.7	La solución debe permitir visualizar un comparativo de las reputaciones asignadas a los archivos ejecutables por parte de las diferentes fuentes de información integradas.
L.8	La solución debe permitir asignar diferentes niveles de reputación a aplicaciones y certificados que se ejecutan en un ambiente con un punto de análisis a nivel local, la difusión de esta asignación debe realizarse en tiempo real mediante un protocolo diseñado para este propósito sin requerir que los agentes realicen un proceso de actualización de firmas o configuraciones.
L.9	En caso de generarse un evento, la comunicación de este debe ser en tiempo real mediante el protocolo de comunicación diseñado para este fin, no debe depender de los ciclos de actualización de eventos a la consola central ni del "llamado/despertar de agentes"
M	**Especificaciones Generales del sistema colaborativo de amenazas de Día 0**
M.1	El modelo de licenciamiento debe ser por nodo, sin importar la cantidad infraestructura de comunicación necesaria (servidores de comunicación o repositorios de reputación)
M.2	La solución debe permitir la instalación de la infraestructura de comunicación y repositorios de reputación de forma, jerárquica, distribuida y en alta disponibilidad sin afectar los costos de licenciamiento o la configuración, a nivel de capacidad, de la consola central.
M.3	La solución al determinar la reputación de un archivo ejecutable, deberá comunicarla al resto de los equipos de usuarios finales con el objetivo de crear una inteligencia de seguridad en la red.
M.4	La solución deberá comunicarse a través de un marco abierto de intercomunicación entre sus distintos componentes, así como permitir a futuro poder integrar otro tipo de tecnologías incluyendo otros fabricantes
M.5	La solución debe permitir crear una línea base de software instalado en las máquinas de usuario final, con el objetivo de reducir falsos positivos.
M.6	La solución debe proveer la reputación de los archivos ejecutables que han sido ejecutados por primera vez en las máquinas de usuario final. En caso de no poder asignar una reputación inicial deberá proteger las máquinas de los usuarios basado en la política de protección establecida por el administrador.
N	**Arquitectura del sistema colaborativo de amenazas de Día 0**
N.1	La arquitectura de la solución debe prevenir no saturar la red de comunicación de la organización a través de un esquema de suscripción/publicación y petición/respuesta.
N.2	La solución debe ser basada en agente y esta deberá ser administrada de forma centralizada.
N.3	La solución debe almacenar y utilizar como información comparativa la información de las fuentes de reputación. Esta información debe ser almacenada en una base de datos centralizada.
N.4	Todos los componentes que forman parte de la arquitectura de la solución, deben comunicarse a través de un marco de intercambio de información asegurado y optimizado.
N.5	Se debe poder armar una arquitectura basada en clústers o stand alone de los

	servidores de administración de comunicaciones sin necesidad de compras adicionales a nivel licenciamiento.
N.6	Las actualizaciones de mantenimiento de la solución se deben poder hacer remotamente y desde una consola de administración centralizada.
N.7	El método de implementación debe ser sencillo y sin necesidad de agregar múltiples componentes por vector de análisis, más allá del servidor de intercambio de mensajes y los repositorios de reputación
N.8	El método de comunicación entre servidor y clientes debe estar armado mediante un "tunel" encriptado en base a claves que permita mantener la seguridad en el ambiente.
N.9	La solución debe poder implementarse en una modalidad que soporte tolerancia a fallo.
N.10	La solución debe ser de fácil adaptación ante una arquitectura deseada con alcance multinacional, independiente de la cantidad de consolas o la arquitectura de comunicación necesaria para este fin.
N.11	La arquitectura debe permitir optimizar el uso de ancho de banda, creando zonas de servicio donde se atiendan localmente las peticiones de los agentes.
N.12	La solución debe permitir las consultas de reputación local por fuera de la organización, a través de internet mediante el mismo protocolo de comunicación establecido para esta infraestructura
N.13	La solución debe permitir la asignación de políticas de forma granular, donde el administrador pueda asignarlas de forma general, local, por localidad o por cada maquina
O	**Performance del sistema colaborativo de amenazas de Día 0**
O.1	Cada servidor de administración de comunicaciones debe soportar técnicamente hasta 100.000 conexiones concurrentes
O.2	En caso de requerir un análisis más exhaustivo con el objetivo de determinar la reputación de un archivo ejecutable, este análisis debe ser en un ambiente externo evitando ocupar el performance de los equipos de usuario final.
O.3	Impacto mínimo de performance en las estaciones de trabajo
O.4	La solución debe estar diseñada mediante un protocolo de intercambio de información que permita escalar hasta redes de hasta millones de conexiones concurrentes
O.5	El tamaño aproximado de los mensajes en cada request/response deberá ser de 2,2Kb
O.6	El tamaño aproximado de los mensajes en cada evento de detección deberá ser de 0,7Kb
P	**Integración del sistema colaborativo de amenazas de Día 0**
P.1	La solución debe poder integrarse mediante el protocolo de comunicación usado dentro de esta arquitectura con la herramienta de análisis de malware avanzado del mismo fabricante, para ofrecer una reputación en base a los resultados que esta analice
P.2	La solución debe poder integrarse con el agente de endpoint security, a fin de poder accionar inteligencia de amenazas
P.3	La solución debe poder integrarse mediante el protocolo de comunicación usado dentro de esta arquitectura con sensores de red del mismo fabricante y de otras marcas a fin de poder tomar control directamente en la red generando bloqueos
P.4	La solución debe permitir integración con herramientas externas mediante la programación de las API
P.5	La solución debe poder integrarse mediante el protocolo de comunicación usado dentro de esta arquitectura a herramientas SIEM
Q	**Gestión del sistema colaborativo de amenazas de Día 0**
Q.1	La solución debe poder ser administrada desde la misma consola de administración que la solución de antivirus.
Q.2	La solución debe soportar la unificación del usuario y contraseña utilizadas por el usuario en el directorio Activo de Microsoft
Q.3	La solución solo debe poder removerse del sistema por un usuario administrador y remotamente.
Q.4	La consola debe permitir diseñar la arquitectura de comunicación de la solución, mediante un editor gráfico.
Q.5	A través de la consola el administrador debe poder visualizar la base de datos de

	reputaciones, así como hacer modificaciones y aplicar políticas de protección.
Q.6	La consola debe permitir visualizar el estado de las máquinas de usuario final administrados, así como las versiones instaladas, estados de comunicación e información de la maquina
Q.7	El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles
Q.8	La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global
R	**Efectividad del sistema colaborativo de amenazas de Día 0**
R.1	La solución debe utilizar como medio de envío de información un protocolo abierto, propietario de la marca, de propósito específico, basado en MQTT para un mejor rendimiento al momento de declarar o recibir reputaciones.
R.2	Los detalles de las amenazas recogidos del malware encontrado en los puntos terminales y gateways de red deben propagarse a través de la capa de intercambio de datos en milisegundos (tiempo real), lo que enseña a todos los componentes de seguridad del mismo fabricante para que inmunicen de forma preventiva contra las amenazas más recientes detectadas.

4. Consola Central de Administración única. Características mínimas.

S	Aspectos Generales de la Consola Central de Administración
S.1	La consola de administración debe estar basada en una configuración cliente servidor que permita la gestión de miles de equipos desde un punto central.
S.2	La consola de administración debe ser una plataforma semiabierta que permita administrar las tecnologías de seguridad de la marca tales como antivirus, control de dispositivos, sistema de prevención de intrusos de host, protección web, además de herramientas de gestión de parches, control energético entre otros.
S.3	La consola de administración debe permitir el monitoreo, gestión y consulta a los puntos terminales mediante tareas en tiempo real.
S.4	La consola de administración debe permitir realizar consultas del estado de conexión de los agentes y obtener resultados en tiempo real.
S.5	La consola de administración debe ser un único punto de referencia para la gestión, configuración de directrices, obtención de logs y reportes de todas las soluciones de seguridad que forman parte del proyecto.
S.6	La consola de administración debe estar diseñada para trabajar de forma nativa en un sistema operativo Windows de 64 bits.
S.7	La consola de administración debe funcionar con Microsoft SQL Server.
S.8	La consola debe soportar grandes despliegues de clientes para solucionar diversos problemas de seguridad en puntos terminales soportando al menos los sistemas operativos Windows para desktop, Windows Server, SUSE, Linux, Mac OS, Android, iOS, Windows Phone.
S.9	La consola de administración debe recolectar información de soluciones de Seguridad Perimetral y Protección de Datos y de Protección de red, así como interactuar con herramientas de correlación de información.
T	Especificaciones Generales de la Consola Central de Administración
T.1	La consola de administración debe contar con un mecanismo que implemente todos

	los componentes de seguridad que se adquirieron como parte de una suite al momento de introducir el número de licencia.
T.2	La consola de administración debe contar con un administrador de descargas que permita actualizar los componentes instalados desde un solo punto
T.3	La consola de administración debe incluir políticas precargadas de configuración de cada uno de los componentes de seguridad instalados y permitir tomarlas como base para personalizar nuevas.
T.4	La consola de administración debe poder instalar de forma centralizada los agentes de administración en todos los equipos del MPF.
T.5	La consola de administración debe esperar la comunicación de los agentes mediante una calendarización de tal forma que esta no genere tráfico hacia la red de forma excesiva para el envío de políticas de configuración.
T.6	La consola de administración debe esperar la comunicación de los agentes mediante una calendarización de tal forma que esta no genere tráfico hacia la red de forma excesiva para el envío de tareas del agente.
T.7	La consola de administración debe funcionar bajo un sistema basado en roles, de tal forma que se puedan crear diferentes usuarios con distintos niveles de privilegios y/o restricciones.
T.8	La consola de administración debe contener la información para auditar las siguientes actividades: • Logeos al servidor de antivirus cambio de perfiles o roles. • Cambio de contraseñas. • Desinstalación de los agentes por eliminación. • Cambios de políticas. • Agregar o borrar sitios, grupos, computadoras, etc. • Renombrar sitios, grupos o máquinas.
T.9	La consola de administración debe contar con la capacidad de instalar de forma remota y sin necesidad de interacción del usuario todos los componentes de seguridad en los clientes que tiene administrados, incluyendo HIPS y Control de Dispositivos
T.10	La consola de administración debe contar con la capacidad de desinstalar de forma remota y sin necesidad de interacción del usuario todos los componentes de seguridad en los clientes que tiene administrados incluyendo HIPS y Control de Dispositivos
T.11	La consola de administración debe conectarse al sitio de actualizaciones de forma automática cada hora verificar nuevas actualizaciones de spam, antivirus, anti-spyware ya sea por https o por FTP
T.12	La consola de administración debe poder distribuir las actualizaciones a usuarios especificados dentro de la plataforma manualmente o por tareas programadas.
T.13	La consola de administración debe contar con la capacidad de definir el nivel de información que le presenta a las consolas locales de cada equipo administrado
T.14	La consola de administración debe permitir especificar etiquetas a los usuarios ya sea pos su sistema operativo o por alguna característica que se defina a fin de poder administrar los equipos de forma más eficiente.
T.15	La consola de administración debe poder clasificar las maquinas por rangos de dirección IP y mascara de red.
T.16	La consola de administración debe contar con la gestión en idioma español e ingles
T.17	La consola de administración debe permitir la creación de repositorios distribuidos de actualizaciones de virus además de las actualizaciones de los componentes instalados.
T.18	La consola de administración debe tener la capacidad de obtener todas las características de hardware de los equipos administrados
T.19	La consola de administración debe permitir a los equipos administrados actualizarse de forma continua a través de un calendario de actualizaciones
T.20	La consola de administración debe contar con un mecanismo de recuperación de desastres que permita la restauración completa a través de un respaldo de la base de datos.
T.21	La consola de administración debe ser accedida desde un navegador web con soporte total de HTML 5 de tal forma que incluso funcione a través de Safari Web Browser

T.22	La consola de administración debe tener la capacidad de identificar en la o las redes protegidas equipos que no son administrados y en caso necesario desplegar el agente de administración.
T.23	La consola de administración debe permitir gestionar y desplegar hasta tres diferentes versiones de un mismo producto a fin de poder cubrir con equipos que soportan versiones legacy, tener la versión general y correr una versión de prueba al mismo tiempo para los diferentes tipos de equipos que administre
T.24	La consola de administración debe trabajar de forma jerárquica por grupos generales, subgrupos e inclusos subgrupos de los subgrupos y aplicar configuraciones y/o tareas generales o particulares.
T.25	La consola de administración debe permitir crear configuraciones por grupo, dominio o maquina sin afectar la estructura.
T.26	La consola de administración debe poder desplegar los agentes y agruparlos en los grupos/subgrupos que se requieran
T.27	La consola de administración debe poder crear URLs para enviar a los usuarios y se instalen los agentes de administración.
T.28	La consola de administración debe permitir la creación de archivos de instalación del agente de gestión para poder ejecutarlo de forma manual por un administrador local
T.29	La consola de administración debe permitir la creación de archivos de instalación del agente de gestión para poder ejecutarlo de forma manual con las credenciales embebidas de tal forma que se pueda instalar en equipos sin privilegios de instalación
U	Arquitectura de la Consola Central de Administración
U.1	La consola de administración debe trabajar con los siguientes componentes: Servidor central de administración: El servidor debe proporcionar directivas de seguridad y tareas a la solución, debe controlar las actualizaciones y debe procesar los eventos correspondientes a todos los sistemas gestionados. Base de datos: Debe ser el componente de almacenamiento central de todos los datos creados y utilizados por la consola central. Debe poder elegir si desea alojar la base de datos en el servidor central de administración o en un sistema independiente, según las necesidades específicas del MPF. Agente: El agente debe recuperar las actualizaciones, debe garantizar la implementación de las tareas, debe implementar las directivas y debe reenviar los eventos correspondientes a cada uno de los sistemas gestionados. Repositorio principal: El repositorio principal debe recuperar actualizaciones y firmas especificadas por el usuario o de sitios de origen definidos por el usuario. Repositorios distribuidos: Deben ser puntos de acceso local ubicados estratégicamente en todo el entorno para que los agentes puedan recibir firmas, actualizaciones e instalaciones de productos reduciendo al máximo las necesidades de ancho de banda. Dependiendo de cuál sea la configuración de su red, debe poder configurar repositorios distribuidos de tipo super agente HTTP, FTP o recurso compartido UNC. Administradores de agentes remotos: debe ser un servidor que se puede instalar en varias ubicaciones de la red para facilitar la gestión de las comunicaciones con los agentes, el equilibrio de carga y las actualizaciones de productos. Los

	administradores de agentes remotos deben estar formados por un servidor Apache y un analizador de eventos. Deben facilitar la gestión de las necesidades de infraestructuras de redes complejas, al proporcionar más control sobre la comunicación agente-servidor. Servidores registrados: se deben poder utilizar para registrar otros servidores con el servidor central de administración. Entre los tipos de servidores registrados se deben incluir: • Servidor LDAP: se debe utilizar para las reglas de asignación de directivas y para permitir la creación automática de cuentas de usuario. • Servidor SNMP: se debe utilizar para recibir una captura SNMP. • Servidor de base de datos: se debe utilizar para ampliar las funciones de las herramientas de generación de informes avanzada proporcionadas con el software de la consola central de administración.
U.2	La consola de administración debe contar con una base de datos que contenga toda la información de agentes, usuarios, productos, configuraciones, tareas, políticas, etc. Además debe contar con módulos que administren la conexión, políticas, tareas y actualizaciones de los clientes, y que se comuniquen directamente a dicha base de datos.
V	Performance de la Consola Central de Administración
V.1	La consola de administración debe tener la capacidad de instalarse en los siguientes sistemas operativos • Windows 2008 R2 • Windows Server 2008 SP2 64 bits o superior • Windows Server 2012 • Windows Server 2012 R2 • Windows 64 bit • Windows 8 and 8.1 (x64)
V.2	La consola de administración debe ser soportada por los siguientes servidores de virtualización. • Microsoft Hyper-V Server 2008 R2 • Microsoft Hyper-V Server 2012 • Microsoft Hyper-V Server 2012 R2 • VMware ESXi 5.0 • VMware ESXi 5.1 • VMware ESXi 5.5
V.3	La consola de administración debe ser soportada por los siguientes navegadores web: • Internet Explorer 8 o posterior • Chrome 17 o posterior • Firefox 10.0 o posterior
V.4	La consola de administración debe soportar los siguientes motores de bases de datos: • Microsoft SQL Server 2008, with Service Pack 1 o posterior. • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014
X	Integración de la Consola Central de Administración
X.1	La consola de administración debe tener la capacidad de integrarse con servidores LDAP
X.2	La consola de administración debe poder integrarse con un servidor de correo electrónico para el envío de notificaciones, alarmas, reportes, etc., a los usuarios administradores o usuarios definidos en la plataforma.
X.3	La consola de administración debe tener la capacidad de integrarse con las soluciones de protección de red como lo son los Network IPS.
X.4	La consola de administración debe tener la posibilidad de tener integración con servidores externos como: • Otros servidores de administración de puntos finales • Servidores de bases de datos remotos

	• Servidores LDAP. • Servidores Syslog.
X.5	La consola de administración debe tener la capacidad de integrar herramientas de control de energía.
X.6	La consola de administración debe tener la capacidad de integrar herramientas de administración de parches.
X.7	La solución debe soportar los siguientes motores de bases de datos: • Microsoft SQL Server 2008, with Service Pack 1 or later • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014
Y	Reportes y Tableros de Control
Y.1	La consola de administración debe proveer reportes predefinidos para cada producto y la capacidad de visualizarlos, editarlos y crear copias para modificarlas, toda esto debe ser posible vía la administración web.
Y.2	La consola de administración debe contar con tableros de control que permita visualizar una o varias soluciones de seguridad.
Y.3	La consola de administración debe permitir la personalización de los tableros de control para cada usuario.
Y.4	La consola de administración debe permitir especificar el tiempo de consulta a la base de datos de los tableros de control que muestran la información de los productos de seguridad administrados.
Y.5	La consola de administración debe incluir tableros de control preconfigurados con lo más importante de cada solución de seguridad.
Y.6	La consola de administración debe permitir la creación de reportes personalizados de las soluciones de seguridad administradas
Y.7	La consola de administración debe permitir incluir el logo personalizado de la (Empresa, dependencia, institución, etc.) en los reportes generados
Y.8	La consola de administración debe poder almacenar logs de actividad tanto en la consola cliente como en la consola central.
Y.9	La consola de administración debe contar con la funcionalidad de generar reportes de manera automática y enviarlos vía correo electrónico de manera programada a los destinatarios deseados.
Y.10	La consola de administración debe tener la capacidad de exportar los reportes generados mínimamente a los formatos PDF, Excel, Word y HTML.

Condiciones generales de la solución:

Total de equipamiento a cubrir:

- 1560 (un mil quinientos sesenta) AIO/PC/Notebook/Servidores Físicos como mínimo
- 50 (cincuenta) Servidores Virtuales como mínimo

Instalación

Se debe proveer la instalación de la solución completa incluyendo la configuración inicial contemplando las siguientes tareas:

- Relevamiento de la infraestructura actual del cliente.
- Desinstalación de la solución actual de antivirus (MS Endpoint Protection).
- Instalación de la solución en todos los equipos del Ministerio Público Fiscal.
- Documentación detallada de los productos de la Solución implementada.
- Transferencia de conocimiento que se hará durante la instalación de la solución.
- Monitoreo de la solución post producción por (2) dos meses presencial de 40 hs. mensuales.

Soporte técnico del Oferente:

El oferente debe establecer un soporte técnico por el plazo de doce (12) meses para toda la solución implementada contados a partir de la fecha de instalación de la solución. El mismo debe ser bajo la modalidad de días hábiles de 8:00 hs a 19:00 hs., telefónicamente, mail o presencial dentro del ámbito de la Ciudad Autónoma de Buenos Aires en caso de ser necesario. El tiempo de respuesta para cada incidente reportado será de no más de cuatro (4) horas. Los técnicos deberán ser certificados en la solución y en caso de necesitar escalar el incidente al fabricante, será el Oferente el encargado de hacerlo, así también como el seguimiento del mismo.

Licenciamiento:

La entrega del producto se hará efectiva mediante alguna de las siguientes opciones:

a) La descarga del producto desde Internet a través de un código.
b) La entrega de sus originales en CD-ROM con sus respectivas licencias y toda la documentación de los mismos.

Las Licencias serán perpetuas con un servicio de soporte del fabricante de 8x5 y actualización de las versiones, bases, definiciones y firmas de virus por doce (12) meses.

Certificado:

Se debe poseer certificación ICSA Labs (www.icsalabs.com), o AVTest (www.av-test.org) para “Empresas Windows Client” que supere o iguale calificaciones de 5.0/6.0 para “Protección”, “Carga del sistema” y “Utilidad”. La calificación indicada debe incluir la fecha de emisión, la que no debe ser mayor a 1 año, y debe corresponder con la versión de software antivirus que se está ofertando para plataforma W10.