INFORME DE EVALUACIÓN PROCESO N° TC-MC-010-2015

En la ciudad de Cartagena de Indias D. T y C., a los veintidós (22) días del mes de Diciembre de 2015, en desarrollo del Proceso de Selección de Mínima Cuantía No. TC-MC-010-2015, que tiene por objeto *Contratar el suministro de una extensión de garantía para el actual servidor PROLIANT ML370 utilizado en la entidad y la adquisición de las 41 licencias de antivirus para los equipos cómputo activos de Transcaribe S.A.*; se procede a verificar los requisitos habilitantes exigidos dentro de la invitación pública del presente proceso; por ello se ha elaborado este documento con el fin de explicar de manera detallada el alcance de la verificación efectuada.

De acuerdo al plazo fijado en la invitación pública se recibió la siguiente propuesta:

Empresa	Valor Propuesta
ACCESAR S.A.S.	$9.579.164

De conformidad con el procedimiento establecido en la Ley 80 de 1993, la Ley 1150 de 2007, ley 1474 de 2011, el Decreto Reglamentario N° 1082 de 2015, se procede a rendir Informe de Evaluación de los requisitos habilitantes (jurídico, técnicos y experiencia) dentro del presente proceso, por parte del Comité Evaluador, en los siguientes términos:

EVALUACIÓN ECONÓMICA

Se procedió a verificar la única propuesta recibida con menor precio, teniendo en cuenta el análisis de sector realizado y como soporte de ello las cotizaciones solicitadas para el análisis y verificación de los precios del mercado; esto con el fin de determinar que el valor ofertado no sobrepasa el presupuesto oficial, ni se encuentra artificialmente bajo, para así proceder a verificar los requisitos habilitantes, presentándose el siguiente resultado:

Precio:

ACCESAR S.A.S.	$9.579.164

Teniendo en cuenta lo estipulado en el artículo 2.2.1.2.1.5.2 del Decreto Reglamentario 1082 de 2015 y en el numeral 12 de la invitación pública, se verificarán los requisitos de la oferta presentada con el menor valor, y que de acuerdo a lo analizado por el comité asesor y evaluador económico, el valor se encuentra ajustado a lo cotizado por el mismo proponente en la etapa precontractual y que sirvió de base para los estudios previos, además de eso y considerando que los márgenes de descuentos sobre la cotización inicial son ínfimos, la propuesta se encuentra habilitada financieramente para ser evaluada por el comité asesor dado que no constituye oferta con precio artificialmente bajo, por ello se considera propuesta hábil y se procede a verificar los requisitos jurídicos de la propuesta presentada por ACCESAR S.A.S., identificada con NIT N° 800.217.129-6, por ser la oferta con el menor precio se analiza lo siguiente:

VERIFICACIÓN DE REQUISITOS HABILITANTES:

- **REQUISITOS HABILITANTES JURÍDICOS**

ACCESAR S.A.S	CUMPLE	NO CUMPLE	OBSERVACIONES
Carta de presentación de la propuesta.	X		Folio 01, 02.
Acta de constitución consorcial o de unión temporal			N/A
Certificado de matricula mercantil			N/A
Certificado De Existencia Y Representación Legal.	X		Folio 03,04 y 05 reverso
Cedula De Ciudadanía Del Oferente O Del Representante Legal en el caso de Personas Jurídicas.	X		Folio - 06
Certificado de antecedentes fiscales	X		Folio 08, la entidad verifica de acuerdo con la ley 962 de 2005, ley 1238 de 2008, circular 5 de 2008.
Certificado de antecedentes disciplinarios	X		Folio 09, la entidad verifica de acuerdo con la ley 962 de 2005, ley 1238 de 2008, circular 5 de 2008.
RUT	X		Folio 011
Constancia que acrediten afiliación y encontrarse al día con el sistema de seguridad social integral	X		Folio 012, se evidencia que la certificación está firmada por el revisor fiscal, señor GUILLERMO CASTRO ORTIZ.
Manifestación de no encontrarse en ninguna causal de inhabilidad e incompatibilidad	X		Folio 07, se evidencia que la manifestación está firmada por el representante legal suplente.
Formato compromiso anticorrupción diligenciado	X		Folio 013 y 014, se evidencia que la manifestación está firmada por el representante legal suplente.
Certificado de antecedentes- Policía Nacional	X		Folio 010, Verificado por la entidad, de acuerdo con la ley 962 de 2005, ley 1238 de 2008, circular 5 de

			2008.

CONCLUSIÓN:

La propuesta presentada por ACCESAR S.A.S., **CUMPLE** con los requisitos habilitantes Jurídicos exigidos en la invitación pública.

Se procede a verificar la experiencia de la empresa, y las especificaciones técnicas ofrecidas de acuerdo a lo señalado en la siguiente tabla:

➢ **REQUISITOS DE EXPERIENCIA**

ACCESAR S.A.S.	CUMPLE	NO CUMPLE	OBSERVACIONES
Experiencia del Proponente: Se acreditará con la presentación de DOS (02) certificaciones de experiencia que acredite la experiencia en contratos similares al objeto de la presente invitación pública, ejecutados satisfactoriamente dentro de los últimos dos (2) anos, contados a partir de la fecha de cierre del presente proceso de selección, expedidas por entidades oficiales y/o privadas con las que haya contratado y cuya sumatoria en valor sea mínimo del 100% del valor del presupuesto oficial estimado para este proceso. La certificación debe contener como mínimo: ./ Entidad contratante . ./ Persona a la que certifica y número de identificación ../ Objeto del contrato. ./ Valor del contrato. ./ Fecha de iniciación y fecha de terminación. ./ Suscripción por parte de la persona que certifica.	X		Filio 016, 017, 018,... 023

CONCLUSIÓN:

La propuesta presentada por ACCESAR S.A.S., **CUMPLE** con los requisitos de experiencia exigidos en la invitación pública.

➢ **ESPECIFICACIONES TÉCNICAS:**

a) UNA (1) EXTENCION DE GARANTIA PARA EL SERVIDOR PROLIANT ML370G4

Descripción	Especificaciones técnicas mínimas.	Resultado
Una extensión de garantía para **SERVIDOR HP PROLIANT ML370G4** Número de Serie (USE611N0B0).	HP SERVIDOR PROLIANT ML370G4 Número de Serie (USE611N0B0).	Folio 028, 029,....039.
Número de Parte del servidor **379912-001**		CUMPLE
Garantía y Soporte:	Desde 01 de Enero hasta 31 de Diciembre de 2016, esta debe cubrir soporte en sitio y dado directamente por el fabricante a nombre de Transcaribe S.A.	CUMPLE
Instalación:	Entregar el documentos que respalda dicha garantía en las oficinas de TRANSCARIBE S.A.	CUMPLE

b) CUARENTA Y UNO (41) LICENCIA DE ANTIVIRUS CON COBERTURA DE SOPORTE Y DERECHO DE ACTUALIZACIÓN DE TRES (3) ANOS.

Descripción	Especificaciones técnicas mínimas.	Resultado
CUARENTA Y UNO (41) LICENCIA DE ANTIVIRUS A NOMBRE DE TRANSCARIBE S.A. CON DERECHO DE ACTUALIZACIÓN DE TRES (3) ANOS.	SERVIDOR DE ADMINISTRACIÓN Y CONSOLA ADMINISTRATIVA CARACTERÍSTICAS DE LA LICENCIA: • ACCESO A LA CONSOLA VÍA WEB (HTTPS) O MMC. • COMPATIBILIDAD CON WINDOWS FAILOVER CLUSTERING U OTRA SOLUCIÓN DE ALTA DISPONIBILIDAD. • CAPACIDAD DE ELIMINAR REMOTAMENTE SOLUCIONES DE PROTECCIÓN DE PUNTO FINAL (PROPIA O DE TERCEROS) QUE ESTÉ PRESENTE EN LAS ESTACIONES Y SERVIDORES. • CAPACIDAD DE INSTALAR REMOTAMENTE LA SOLUCIÓN DE PROTECCIÓN DE PUNTO FINAL EN LAS ESTACIONES Y SERVIDORES WINDOWS, A TRAVÉS DE LA ADMINISTRACIÓN COMPARTIDA, LOGIN SCRIPT Y/O	CUMPLE, FOLIO 040, 041.

	GPO DE ACTIVE DIRECTORY. • CAPACIDAD DE INSTALAR REMOTAMENTE LA SOLUCIÓN DE SEGURIDAD EN SMARTPHONES Y TABLETS ANDROID, IOS Y WPHONE, UTILIZANDO ESTACIONES COMO INTERMEDIADORAS. • CAPACIDAD DE INSTALAR REMOTAMENTE APLICACIONES "APP" EN SMARTPHONES Y TABLETS DE SISTEMA IOS. • CAPACIDAD DE GESTIONAR ESTACIONES DE TRABAJO Y SERVIDORES DE ARCHIVOS (TANTO WINDOWS COMO LINUX Y MAX) PROTEGIDOS POR LA SOLUCIÓN ANTIVIRUS. • CAPACIDAD DE GESTIONAR SMARTPHONES Y TABLETS (TANTO WINDOWS PHONE, ANDROID Y IOS) Y LOS PROTEGIDOS POR LA SOLUCIÓN ANTIVIRUS (ANDROID). • CAPACIDAD DE GENERAR PAQUETES PERSONALIZADOS (AUTOEJECUTABLES) CONTENIENDO LA LICENCIA Y CONFIGURACIONES DEL PRODUCTO. • CAPACIDAD DE ACTUALIZAR LOS PAQUETES DE INSTALACIÓN CON LAS ÚLTIMAS VACUNAS, PARA QUE CUANDO EL PAQUETE SEA UTILIZADO EN UNA INSTALACIÓN YA CONTENGA LAS ÚLTIMAS VACUNAS LANZADAS. • CAPACIDAD DE HACER DISTRIBUCIÓN REMOTA DE CUALQUIER SOFTWARE, O SEA, DEBE SER CAPAZ DE ENVIAR REMOTAMENTE CUALQUIER SOFTWARE POR LA ESTRUCTURA DE GERENCIAMIENTO DE ANTIVIRUS PARA QUE SEA INSTALADO EN LAS MÁQUINAS CLIENTES. • CAPACIDAD DE DESINSTALAR REMOTAMENTE APLICACIONES INSTALADAS EN LAS MÁQUINAS CLIENTES. • CAPACIDAD DE APLICAR ACTUALIZACIONES DE WINDOWS REMOTAMENTE EN LAS ESTACIONES Y SERVIDORES. • CAPACIDAD DE IMPORTAR LA ESTRUCTURA DE ACTIVE DIRECTORY PARA ENCONTRAR MÁQUINAS.	

	• CAPACIDAD DE MONITOREAR DIFERENTES SUBNETS DE RED CON EL OBJETIVO DE ENCONTRAR MÁQUINAS NUEVAS PARA QUE SEAN AGREGADAS A LA PROTECCIÓN. • CAPACIDAD DE MONITOREAR GRUPOS DE TRABAJOS YA EXISTENTES Y CUALQUIER GRUPO DE TRABAJO QUE SEA CREADO EN LA RED, CON EL OBJETIVO DE ENCONTRAR MÁQUINAS NUEVAS PARA SER AGREGADAS A LA PROTECCIÓN. • CAPACIDAD DE QUE CUANDO SE DETECTEN MÁQUINAS NUEVAS EN EL ACTIVE DIRECTORY, SUBNETS O GRUPOS DE TRABAJO, AUTOMÁTICAMENTE SE IMPORTE LA MÁQUINA PARA LA ESTRUCTURA DE PROTECCIÓN DE LA CONSOLA Y SE VERIFIQUE SI TIENE EL ANTIVIRUS INSTALADO. EN CASO DE NO TENERLO, DEBE INSTALAR EL ANTIVIRUS AUTOMÁTICAMENTE. • CAPACIDAD DE AGRUPAMIENTO DE MÁQUINAS POR CARACTERÍSTICAS COMUNES ENTRE ELLAS, POR EJEMPLO: AGRUPAR TODAS LAS MÁQUINAS QUE NO TENGAN EL ANTIVIRUS INSTALADO, AGRUPAR TODAS LAS MÁQUINAS QUE NO RECIBIERON ACTUALIZACIÓN EN LOS ÚLTIMOS 2 DÍAS, ETC. • CAPACIDAD DE DEFINIR POLÍTICAS DE CONFIGURACIONES DIFERENTES POR GRUPOS DE ESTACIONES, PERMITIENDO QUE SEAN CREADOS SUBGRUPOS Y CON FUNCIÓN DE HERENCIA DE POLÍTICAS ENTRE GRUPOS Y SUBGRUPOS. • DEBE PROPORCIONAR LA SIGUIENTE INFORMACIÓN DE LAS COMPUTADORAS: O SI EL ANTIVIRUS ESTÁ INSTALADO. O SI EL ANTIVIRUS HA INICIADO. O SI EL ANTIVIRUS ESTÁ ACTUALIZADO; O MINUTOS/HORAS DESDE LA ÚLTIMA CONEXIÓN DE LA MÁQUINA CON EL SERVIDOR ADMINISTRATIVO; O MINUTOS/HORAS DESDE LA ÚLTIMA ACTUALIZACIÓN DE VACUNAS.	

	O FECHA Y HORARIO DE LA ÚLTIMA VERIFICACIÓN EJECUTADA EN LA MÁQUINA; O VERSIÓN DEL ANTIVIRUS INSTALADO EN LA MÁQUINA; O SI ES NECESARIO REINICIAR LA COMPUTADORA PARA APLICAR CAMBIOS; O FECHA Y HORARIO DE CUANDO LA MÁQUINA FUE ENCENDIDA; O CANTIDAD DE VIRUS ENCONTRADOS (CONTADOR) EN LA MÁQUINA; O NOMBRE DE LA COMPUTADORA; O DOMINIO O GRUPO DE TRABAJO DE LA COMPUTADORA; O FECHA Y HORARIO DE LA ÚLTIMA ACTUALIZACIÓN DE VACUNAS; O SISTEMA OPERATIVO CON SERVICE PACK; O CANTIDAD DE PROCESADORES; O CANTIDAD DE MEMORIA RAM; O USUARIO(S) CONECTADOS EN ESE MOMENTO, CON INFORMACIÓN DE CONTACTO (SI ESTÁN DISPONIBLES EN EL ACTIVE DIRECTORY) O DIRECCIÓN IP; O APLICATIVOS INSTALADOS, INCLUSIVE APLICATIVOS DE TERCEROS, CON HISTORIAL DE INSTALACIÓN, CONTENIENDO FECHA Y HORA EN QUE EL SOFTWARE FUE INSTALADO O REMOVIDO. O ACTUALIZACIONES DE WINDOWS UPDATES INSTALADAS. O INFORMACIÓN COMPLETA DE HARDWARE CONTENIENDO: PROCESADORES, MEMORIA, ADAPTADORES DE VIDEO, DISCOS DE ALMACENAMIENTO, ADAPTADORES DE AUDIO, ADAPTADORES DE RED, MONITORES, DRIVES DE CD/DVD O VULNERABILIDADES DE APLICATIVOS	

	INSTALADOS EN LA MÁQUINA O DEBE PERMITIR BLOQUEAR LAS CONFIGURACIONES DEL ANTIVIRUS INSTALADO EN LAS ESTACIONES Y SERVIDORES DE MANERA QUE EL USUARIO NO LOGRE MODIFICARLAS; • CAPACIDAD DE REUBICAR MÁQUINAS CLIENTES, BASADO EN REGLAS DE CONEXIÓN COMO: O CAMBIO DE GATEWAY; O CAMBIO DE SUBNET DNS; O CAMBIO DE DOMINIO; O CAMBIO DE SERVIDOR DHCP; O CAMBIO DE SERVIDOR DNS; O CAMBIO DE SERVIDOR WINS; O APARICIÓN DE NUEVA SUBNET; • CAPACIDAD DE CONFIGURAR POLÍTICAS MÓVILES PARA QUE CUANDO UNA COMPUTADORA CLIENTE ESTÉ FUERA DE LA ESTRUCTURA DE PROTECCIÓN PUEDA ACTUALIZARSE VÍA INTERNET; • CAPACIDAD DE INSTALAR OTROS SERVIDORES ADMINISTRATIVOS PARA BALANCEAR LA CARGA Y OPTIMIZAR EL TRÁFICO DE ENLACES ENTRE SITIOS DIFERENTES; • CAPACIDAD DE INTERRELACIONAR SERVIDORES EN ESTRUCTURA DE JERARQUÍA PARA OBTENER INFORMES SOBRE TODA LA ESTRUCTURA DE ANTIVIRUS; • CAPACIDAD DE HERENCIA DE TAREAS Y POLÍTICAS EN LA ESTRUCTURA JERÁRQUICA DE SERVIDORES ADMINISTRATIVOS; • CAPACIDAD DE ELEGIR CUALQUIER COMPUTADORA CLIENTE COMO REPOSITORIO DE VACUNAS Y DE PAQUETES DE INSTALACIÓN, SIN QUE SEA NECESARIO LA INSTALACIÓN DE UN SERVIDOR ADMINISTRATIVO COMPLETO, DONDE OTRAS MÁQUINAS CLIENTES SE ACTUALIZARÁN Y RECIBIRÁN PAQUETES DE INSTALACIÓN, CON EL FIN DE	

	OPTIMIZAR EL TRÁFICO DE RED; • CAPACIDAD DE HACER DE ESTE REPOSITORIO DE VACUNAS UN GATEWAY PARA CONEXIÓN CON EL SERVIDOR DE ADMINISTRACIÓN, PARA QUE OTRAS MÁQUINAS QUE NO LOGRAN CONECTARSE DIRECTAMENTE AL SERVIDOR PUEDAN USAR ESTE GATEWAY PARA RECIBIR Y ENVIAR INFORMACIÓN AL SERVIDOR ADMINISTRATIVO. • CAPACIDAD DE EXPORTAR INFORMES PARA LOS SIGUIENTES TIPOS DE ARCHIVOS: PDF, HTML Y XML. • CAPACIDAD DE GENERAR TRAPS SNMP PARA MONITOREO DE EVENTOS; • CAPACIDAD DE ENVIAR CORREOS ELECTRÓNICOS PARA CUENTAS ESPECÍFICAS EN CASO DE ALGÚN EVENTO; • DEBE TENER COMPATIBILIDAD CON MICROSOFT NAP, CUANDO SE INSTALE EN UN WINDOWS 2008 SERVER; • DEBE TENER COMPATIBILIDAD CON CISCO NETWORK ADMISSION CONTROL (NAC); • DEBE TENER DOCUMENTACIÓN DE LA ESTRUCTURA DEL BANCO DE DATOS PARA GENERAR INFORMES A PARTIR DE HERRAMIENTAS ESPECÍFICAS DE CONSULTA (CRYSTAL REPORTS, POR EJEMPLO). • CAPACIDAD DE ENCENDER MÁQUINAS VÍA WAKE ON LAN PARA REALIZAR TAREAS (BARRIDO, ACTUALIZACIÓN, INSTALACIÓN, ETC.), INCLUSIVE DE MÁQUINAS QUE ESTÉN EN SUBNETS DIFERENTES DEL SERVIDOR); • CAPACIDAD DE HABILITAR AUTOMÁTICAMENTE UNA POLÍTICA EN CASO DE QUE OCURRA UNA EPIDEMIA EN LA RED (BASADO EN CANTIDAD DE VIRUS ENCONTRADOS EN DETERMINADO INTERVALO DE TIEMPO); • CAPACIDAD DE REALIZAR ACTUALIZACIÓN INCREMENTAL DE VACUNAS EN LAS COMPUTADORAS CLIENTES; • CAPACIDAD DE REPORTAR	

	VULNERABILIDADES DE SOFTWARE PRESENTES EN LAS COMPUTADORAS. • CAPACIDAD DE REALIZAR INVENTARIO DE HARDWARE DE TODAS LAS MÁQUINAS CLIENTES; • CAPACIDAD DE REALIZAR INVENTARIO DE APLICATIVOS INSTALADOS EN TODAS LAS MÁQUINAS CLIENTES; • CAPACIDAD DE DIFERENCIAR MÁQUINAS VIRTUALES DE MÁQUINAS FÍSICAS; • DEBE PERMITIR INTEGRACIÓN CON HERRAMIENTAS SIEM LÍDERES DEL MERCADO: HP ARCSIGHT E IBM QRADAR • CARACTERÍSTICAS DEL SISTEMA DE PROTECCIÓN INCLUIDAS EN UN SOLO MÓDULO DE INSTALACIÓN: • DEBE PROPORCIONAR LAS SIGUIENTES PROTECCIONES: O ANTIVIRUS DE ARCHIVOS RESIDENTE (ANTISPYWARE, ANTITROYANO, ANTIMALWARE, ETC.) QUE VERIFIQUE CUALQUIER ARCHIVO CREADO, ACCEDIDO O MODIFICADO; O ANTIVIRUS DE WEB (MÓDULO PARA VERIFICACIÓN DE SITIOS Y DOWNLOADS CONTRA VIRUS) O ANTIVIRUS DE CORREO ELECTRÓNICO (MÓDULO PARA VERIFICACIÓN DE CORREOS RECIBIDOS Y ENVIADOS, ASÍ COMO SUS ADJUNTOS) O ANTIVIRUS DE MENSAJES INSTANTÁNEOS (MÓDULO PARA VERIFICACIÓN DE MENSAJES INSTANTÁNEOS, COMO ICQ, MSN, IRC, ETC.) O FIREWALL CON IDS O AUTOPROTECCIÓN (CONTRA ATAQUES A LOS SERVICIOS/PROCESOS DEL ANTIVIRUS) O CONTROL DE DISPOSITIVOS EXTERNOS O CONTROL DE ACCESO A SITIOS POR CATEGORÍA	

	O CONTROL DE EJECUCIÓN DE APLICATIVOS POR NEGACIÓN POR DEFECTO (DEFAULT DENY) O INFORMACIÓN DE VULNERABILIDADES DE WINDOWS Y DE LOS APLICATIVOS INSTALADOS O CAPACIDAD DE ELEGIR DE QUÉ MÓDULOS SE INSTALARÁN, TANTO EN LA INSTALACIÓN LOCAL COMO EN LA INSTALACIÓN REMOTA; O LAS VACUNAS DEBEN SER ACTUALIZADAS POR EL FABRICANTE Y ESTAR DISPONIBLES A LOS USUARIOS, COMO MÁXIMO CADA HORA, INDEPENDIENTEMENTE DEL NIVEL DE LAS AMENAZAS ENCONTRADAS EN EL PERÍODO (ALTO, MEDIO O BAJO). O CAPACIDAD DE DETECCIÓN DE PRESENCIA DE ANTIVIRUS DE OTRO FABRICANTE QUE PUEDA CAUSAR INCOMPATIBILIDAD, BLOQUEANDO LA INSTALACIÓN; O CAPACIDAD DE AGREGAR CARPETAS/ARCHIVOS PARA UNA ZONA DE EXCLUSIÓN, CON EL FIN DE EXCLUIRLOS DE LA VERIFICACIÓN. CAPACIDAD, TAMBIÉN, DE AGREGAR OBJETOS A LA LISTA DE EXCLUSIÓN DE ACUERDO CON EL RESULTADO DEL ANTIVIRUS, (EJ.: "WIN32.TROJAN.BANKER") PARA QUE CUALQUIER OBJETO DETECTADO CON EL RESULTADO ELEGIDO SEA IGNORADO; O CAPACIDAD DE AGREGAR APLICATIVOS A UNA LISTA DE "APLICATIVOS CONFIABLES", DONDE LAS ACTIVIDADES DE RED, ACTIVIDADES DE DISCO Y ACCESO AL REGISTRO DE WINDOWS NO SERÁN MONITOREADAS; O POSIBILIDAD DE DESHABILITAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS CUANDO LA COMPUTADORA ESTÉ FUNCIONANDO MEDIANTE BATERÍAS (NOTEBOOKS); O CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS EN CASO DE QUE OTROS APLICATIVOS NECESITEN MÁS RECURSOS DE MEMORIA O PROCESAMIENTO; O CAPACIDAD DE VERIFICAR ARCHIVOS POR	

	CONTENIDO, O SEA, ÚNICAMENTE VERIFICARÁ EL ARCHIVO SI ES POSIBLE DE INFECCIÓN. EL ANTIVIRUS DEBE ANALIZAR LA INFORMACIÓN DE ENCABEZADO DEL ARCHIVO PARA TOMAR O NO ESA DECISIÓN A PARTIR DE LA EXTENSIÓN DEL ARCHIVO; O CAPACIDAD DE VERIFICAR SOLAMENTE ARCHIVOS NUEVOS Y MODIFICADOS; O CAPACIDAD DE VERIFICAR OBJETOS USANDO HEURÍSTICA; O CAPACIDAD DE AGENDAR UNA PAUSA EN LA VERIFICACIÓN; O CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE LA VERIFICACIÓN CUANDO SE INICIE UN APLICATIVO; • EL ANTIVIRUS DE ARCHIVOS, AL ENCONTRAR UN OBJETO POTENCIALMENTE PELIGROSO, DEBE: O PREGUNTAR QUÉ HACER, O; O BLOQUEAR EL ACCESO AL OBJETO; O BORRAR EL OBJETO O INTENTAR DESINFECTARLO (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); O CASO POSITIVO DE DESINFECCIÓN: O RESTAURAR EL OBJETO PARA USO; O CASO NEGATIVO DE DESINFECCIÓN: O MOVER PARA CUARENTENA O BORRAR (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); O ANTERIORMENTE A CUALQUIER INTENTO DE DESINFECCIÓN O EXCLUSIÓN PERMANENTE, EL ANTIVIRUS DEBE REALIZAR UN RESPALDO DEL OBJETO. O CAPACIDAD DE VERIFICAR CORREOS ELECTRÓNICOS RECIBIDOS Y ENVIADOS EN LOS PROTOCOLOS POP3, IMAP, NNTP, SMTP Y MAPI, ASÍ COMO CONEXIONES CIFRADAS (SSL) PARA POP3 Y IMAP (SSL);	

	O CAPACIDAD DE VERIFICAR TRÁFICO DE ICQ, MSN, AIM Y IRC CONTRA VIRUS Y ENLACES PHISHINGS; O CAPACIDAD DE VERIFICAR ENLACES INTRODUCIDOS EN CORREOS ELECTRÓNICOS CONTRA PISHINGS; O CAPACIDAD DE VERIFICAR TRÁFICO SSL EN LOS BROWSERS: INTERNET EXPLORER, FIREFOX Y OPERA; O CAPACIDAD DE VERIFICACIÓN DEL CUERPO DEL CORREO ELECTRÓNICO Y ADJUNTOS USANDO HEURÍSTICA; • EL ANTIVIRUS DE CORREOS ELECTRÓNICOS, AL ENCONTRAR UN OBJETO POTENCIALMENTE PELIGROSO DEBE: O PREGUNTAR QUÉ HACER, O; O BLOQUEAR EL CORREO ELECTRÓNICO; O BORRAR EL OBJETO O INTENTAR DESINFECTARLO (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); O CASO POSITIVO DE DESINFECCIÓN: • RESTAURAR EL CORREO ELECTRÓNICO PARA EL USUARIO; • CASO NEGATIVO DE DESINFECCIÓN: • MOVER PARA CUARENTENA O BORRAR EL OBJETO (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); • EN CASO DE QUE EL CORREO ELECTRÓNICO CONTENGA CÓDIGO QUE PARECE SER, PERO NO ES DEFINITIVAMENTE MALICIOSO, ESTE DEBE MANTENERSE EN CUARENTENA. O POSIBILIDAD DE VERIFICAR SOLAMENTE CORREOS ELECTRÓNICOS RECIBIDOS, O RECIBIDOS Y ENVIADOS. O CAPACIDAD DE FILTRAR ADJUNTOS DE	

	CORREOS ELECTRÓNICOS, BORRÁNDOLOS O RENOMBRÁNDOLOS DE ACUERDO CON LA CONFIGURACIÓN HECHA POR EL ADMINISTRADOR. O CAPACIDAD DE VERIFICACIÓN DE TRÁFICO HTTP Y CUALQUIER SCRIPT DE WINDOWS SCRIPT HOST (JAVASCRIPT, VISUAL BASIC SCRIPT, ETC.), USANDO HEURÍSTICAS; O DEBE TENER SOPORTE TOTAL AL PROTOCOLO IPV6; O CAPACIDAD DE MODIFICAR LAS PUERTAS MONITOREADAS POR LOS MÓDULOS DE WEB Y CORREO ELECTRÓNICO; O EN LA VERIFICACIÓN DE TRÁFICO WEB, EN CASO DE QUE SE ENCUENTRE CÓDIGO MALICIOSO EL PROGRAMA DEBE: • PREGUNTAR QUÉ HACER, O; • BLOQUEAR EL ACCESO AL OBJETO Y MOSTRAR UN MENSAJE SOBRE EL BLOQUEO, O; • PERMITIR ACCESO AL OBJETO; O EL ANTIVIRUS DE WEB DEBE REALIZAR LA VERIFICACIÓN DE, COMO MÍNIMO, DOS MANERAS DIFERENTES, A ELECCIÓN DEL ADMINISTRADOR: O VERIFICACIÓN ON-THE-FLY, DONDE SE VERIFICAN LOS DATOS MIENTRAS SON RECIBIDOS EN TIEMPO REAL, O; O VERIFICACIÓN DE BUFFER, DONDE LOS DATOS SE RECIBEN Y SON ALMACENADOS PARA POSTERIOR VERIFICACIÓN. O POSIBILIDAD DE AGREGAR SITIOS DE LA WEB EN UNA LISTA DE EXCLUSIÓN, DONDE NO SERÁN VERIFICADOS POR EL ANTIVIRUS DE WEB. O DEBE TENER MÓDULO QUE ANALICE LAS ACCIONES DE CADA APLICACIÓN EN EJECUCIÓN EN LA COMPUTADORA, GRABANDO LAS ACCIONES EJECUTADAS Y COMPARÁNDOLAS CON SECUENCIAS CARACTERÍSTICAS DE ACTIVIDADES PELIGROSAS. TALES REGISTROS DE SECUENCIAS DEBEN SER	

	ACTUALIZADOS CONJUNTAMENTE CON LAS VACUNAS. O DEBE TENER MÓDULO QUE ANALICE CADA MACRO DE VBA EJECUTADO, BUSCANDO POR SEÑALES DE ACTIVIDAD MALICIOSA. O DEBE TENER MÓDULO QUE ANALICE CUALQUIER INTENTO DE EDICIÓN, EXCLUSIÓN O GRABACIÓN DEL REGISTRO, DE FORMA QUE SEA POSIBLE ELEGIR CLAVES ESPECÍFICAS PARA SER MONITOREADAS Y/O BLOQUEADAS. O DEBE TENER MÓDULO DE BLOQUEO DE PHISHING, CON ACTUALIZACIONES INCLUIDAS EN LAS VACUNAS, OBTENIDAS POR ANTI-PHISHING WORKING GROUP (HTTP://WWW.ANTIPHISHING.ORG/). O CAPACIDAD DE DISTINGUIR DIFERENTES SUBNETS Y BRINDAR OPCIÓN DE ACTIVAR O NO EL FIREWALL PARA UNA SUBNET ESPECÍFICA; O DEBE TENER MÓDULO IDS (INTRUSION DETECTION SYSTEM) PARA PROTECCIÓN CONTRA PORT SCANS Y EXPLOTACIÓN DE VULNERABILIDADES DE SOFTWARE. LA BASE DE DATOS DE ANÁLISIS DEBE ACTUALIZARSE CONJUNTAMENTE CON LAS VACUNAS. O EL MÓDULO DE FIREWALL DEBE CONTENER, COMO MÍNIMO, DOS CONJUNTOS DE REGLAS: O FILTRADO DE PAQUETES: DONDE EL ADMINISTRADOR PODRÁ ELEGIR PUERTAS, PROTOCOLOS O DIRECCIONES DE CONEXIÓN QUE SERÁN BLOQUEADAS/PERMITIDAS; O FILTRADO POR APLICATIVO: DONDE EL ADMINISTRADOR PODRÁ ELEGIR CUÁL APLICATIVO, GRUPO DE APLICATIVO, FABRICANTE DE APLICATIVO, VERSIÓN DE APLICATIVO O NOMBRE DE APLICATIVO TENDRÁ ACCESO A LA RED, CON LA POSIBILIDAD DE ELEGIR QUÉ PUERTAS Y PROTOCOLOS PODRÁN SER UTILIZADOS. O DEBE TENER MÓDULO QUE HABILITE O NO EL FUNCIONAMIENTO DE LOS SIGUIENTES DISPOSITIVOS EXTERNOS, COMO MÍNIMO: • DISCOS DE ALMACENAMIENTO LOCALES	

	• ALMACENAMIENTO EXTRAÍBLE • IMPRESORAS • CD/DVD • DRIVES DE DISQUETE • MODEMS • DISPOSITIVOS DE CINTA • DISPOSITIVOS MULTIFUNCIONALES • LECTORES DE SMART CARD • WI-FI • ADAPTADORES DE RED EXTERNOS • DISPOSITIVOS MP3 O SMARTPHONES • DISPOSITIVOS BLUETOOTH O CAPACIDAD DE LIBERAR ACCESO A UN DISPOSITIVO ESPECÍFICO Y USUARIOS ESPECÍFICOS POR UN PERÍODO DE TIEMPO ESPECÍFICO, SIN LA NECESIDAD DE DESHABILITAR LA PROTECCIÓN, SIN DESHABILITAR EL GERENCIAMIENTO CENTRAL O DE INTERVENCIÓN LOCAL DEL ADMINISTRADOR EN LA MÁQUINA DEL USUARIO. O CAPACIDAD DE LIMITAR LA ESCRITURA Y LECTURA EN DISPOSITIVOS DE ALMACENAMIENTO EXTERNO POR USUARIO. O CAPACIDAD DE LIMITAR LA ESCRITURA Y LECTURA EN DISPOSITIVOS DE ALMACENAMIENTO EXTERNO POR AGENDAMIENTO. O CAPACIDAD DE CONFIGURAR NUEVOS DISPOSITIVOS POR CLASS ID/HARDWARE ID O CAPACIDAD DE LIMITAR EL ACCESO A SITIOS DE INTERNET POR CATEGORÍA, POR CONTENIDO (VIDEO, AUDIO, ETC), CON POSIBILIDAD DE CONFIGURACIÓN POR USUARIO O GRUPOS DE USUARIOS Y AGENDAMIENTO. O CAPACIDAD DE LIMITAR LA EJECUCIÓN DE APLICATIVOS POR HASH MD5, NOMBRE DEL ARCHIVO,	

	VERSIÓN DEL ARCHIVO, NOMBRE DEL APLICATIVO, VERSIÓN DEL APLICATIVO, FABRICANTE/DESARROLLADOR, CATEGORÍA (EJ.: NAVEGADORES, GERENCIADOR DE DOWNLOAD, JUEGOS, APLICACIÓN DE ACCESO REMOTO, ETC). O CAPACIDAD DE BLOQUEAR LA EJECUCIÓN DE UN APLICATIVO QUE ESTÉ EN ALMACENAMIENTO EXTERNO. O CAPACIDAD DE LIMITAR EL ACCESO DE LOS APLICATIVOS A RECURSOS DEL SISTEMA, COMO CLAVES DE REGISTRO Y CARPETAS/ARCHIVOS DEL SISTEMA, POR CATEGORÍA, FABRICANTE O NIVEL DE CONFIANZA DEL APLICATIVO. O CAPACIDAD DE, EN CASO DE EPIDEMIA, ACTIVAR UNA POLÍTICA ALTERNATIVA DONDE CUALQUIER CONFIGURACIÓN PUEDA SER MODIFICADA, DESDE REGLAS DE FIREWALL HASTA CONTROL DE APLICATIVOS, DISPOSITIVOS Y ACCESO A WEB. O CAPACIDAD DE, EN CASO DE QUE LA COMPUTADORA CLIENTE SALGA DE LA RED CORPORATIVA, ACTIVAR UNA POLÍTICA ALTERNATIVA DONDE CUALQUIER CONFIGURACIÓN PUEDA SER MODIFICADA, DESDE REGLAS DE FIREWALL HASTA CONTROL DE APLICATIVOS, DISPOSITIVOS Y ACCESO A WEB. • ESTACIONES Y SERVIDORES MAC OS X – • COMPATIBILIDAD: ▯ MAC OS X 10.4.11 O SUPERIOR ▯ MAC OS X SERVER 10.6, 10.7, 10.8, 10.9, 10.10 O CARACTERÍSTICAS: ▯ DEBE PROPORCIONAR PROTECCIÓN RESIDENTE PARA ARCHIVOS (ANTISPYWARE, ANTITROJANO, ANTIMALWARE, ETC.) QUE VERIFIQUE CUALQUIER ARCHIVO CREADO, ACCEDIDO O MODIFICADO; ▯ CAPACIDAD DE ELEGIR DE QUÉ MÓDULOS SE	

	INSTALARÁN, TANTO EN LA INSTALACIÓN LOCAL COMO EN LA INSTALACIÓN REMOTA; ▯ LA INSTALACIÓN Y PRIMERA EJECUCIÓN DEL PRODUCTO DEBE SER REALIZADA SIN NECESIDAD DE REINICIAR LA COMPUTADORA, DE MODO QUE EL PRODUCTO FUNCIONE CON TODA SU CAPACIDAD; ▯ DEBE CONTAR CON SOPORTES A NOTIFICACIONES UTILIZANDO GROWL; ▯ LAS VACUNAS DEBEN SER ACTUALIZADAS POR EL FABRICANTE Y ESTAR DISPONIBLES A LOS USUARIOS, COMO MÁXIMO CADA HORA, INDEPENDIENTEMENTE DEL NIVEL DE LAS AMENAZAS ENCONTRADAS EN EL PERÍODO (ALTO, MEDIO O BAJO). ▯ CAPACIDAD DE VOLVER A LA BASE DE DATOS DE LA VACUNA ANTERIOR; ▯ CAPACIDAD DE BARRER LA CUARENTENA AUTOMÁTICAMENTE DESPUÉS DE CADA ACTUALIZACIÓN DE VACUNAS; ▯ CAPACIDAD DE AGREGAR CARPETAS/ARCHIVOS PARA UNA ZONA DE EXCLUSIÓN, CON EL FIN DE EXCLUIRLOS DE LA VERIFICACIÓN. CAPACIDAD, TAMBIÉN, DE AGREGAR OBJETOS A LA LISTA DE EXCLUSIÓN DE ACUERDO CON EL RESULTADO DEL ANTIVIRUS, (EJ.:"WIN32.TROJAN.BANKER") PARA QUE CUALQUIER OBJETO DETECTADO CON EL RESULTADO ELEGIDO SEA IGNORADO; ▯ POSIBILIDAD DE DESHABILITAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS CUANDO LA COMPUTADORA ESTÉ FUNCIONANDO MEDIANTE BATERÍAS (NOTEBOOKS); ▯ CAPACIDAD DE VERIFICAR ARCHIVOS POR CONTENIDO, O SEA, ÚNICAMENTE VERIFICARÁ EL ARCHIVO SI ES PASIBLE DE INFECCIÓN. EL ANTIVIRUS DEBE ANALIZAR LA INFORMACIÓN DE ENCABEZADO DEL ARCHIVO PARA TOMAR O NO ESA DECISIÓN A PARTIR DE LA EXTENSIÓN DEL ARCHIVO; ▯ CAPACIDAD DE VERIFICAR SOLAMENTE	

	ARCHIVOS NUEVOS Y MODIFICADOS; ▯ CAPACIDAD DE VERIFICAR OBJETOS USANDO HEURÍSTICA; ▯ CAPACIDAD DE AGENDAR UNA PAUSA EN LA VERIFICACIÓN; ▯ EL ANTIVIRUS DE ARCHIVOS, AL ENCONTRAR UN OBJETO POTENCIALMENTE PELIGROSO, DEBE: • PREGUNTAR QUÉ HACER, O; • BLOQUEAR EL ACCESO AL OBJETO; O BORRAR EL OBJETO O INTENTAR DESINFECTARLO (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); O CASO POSITIVO DE DESINFECCIÓN: ▯ RESTAURAR EL OBJETO PARA USO; O CASO NEGATIVO DE DESINFECCIÓN: ▯ MOVER PARA CUARENTENA O BORRAR (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); ▯ ANTERIORMENTE A CUALQUIER INTENTO DE DESINFECCIÓN O EXCLUSIÓN PERMANENTE, EL ANTIVIRUS DEBE REALIZAR UN RESPALDO DEL OBJETO; ▯ CAPACIDAD DE VERIFICAR ARCHIVOS DE FORMATO DE CORREO ELECTRÓNICO; ▯ POSIBILIDAD DE TRABAJAR CON EL PRODUCTO POR LA LÍNEA DE COMANDO, CON COMO MÍNIMO OPCIONES PARA ACTUALIZAR LAS VACUNAS, INICIAR UN BARRIDO, PARA EL ANTIVIRUS E INICIAR EL ANTIVIRUS POR LA LÍNEA DE COMANDO; ▯ CAPACIDAD DE SER INSTALADO, REMOVIDO Y ADMINISTRADO POR LA MISMA CONSOLA CENTRAL DE GERENCIAMIENTO; • ESTACIONES DE TRABAJO LINUX –	

	O COMPATIBILIDAD (O SUPERIOR):	
	▯ PLATAFORMA 32-BITS:	
	• CANAIMA 3	
	• RED FLAG DESKTOP 6.0 SP2	
	• RED HAT ENTERPRISE LINUX 5.8 DESKTOP	
	• RED HAT ENTERPRISE LINUX 6.2 DESKTOP	
	• FEDORA 16	
	• CENTOS-6.2	
	• SUSE LINUX ENTERPRISE DESKTOP 10 SP4	
	• SUSE LINUX ENTERPRISE DESKTOP 11 SP2	
	• OPENSUSE LINUX 12.1	
	• OPENSUSE LINUX 12.2	
	• DEBIAN GNU/LINUX 6.0.5	
	• MANDRIVA LINUX 2011	
	• UBUNTU 10.04 LTS	
	• UBUNTU 12.04 LTS	
	▯ PLATAFORMA 64-BITS:	
	• CANAIMA 3	
	• RED FLAG DESKTOP 6.0 SP2	
	• RED HAT ENTERPRISE LINUX 5.8	
	• RED HAT ENTERPRISE LINUX 6.2 DESKTOP	
	• FEDORA 16	
	• CENTOS-6.2	
	• SUSE LINUX ENTERPRISE DESKTOP 10 SP4	
	• SUSE LINUX ENTERPRISE DESKTOP 11 SP2	
	• OPENSUSE LINUX 12.1	
	• OPENSUSE LINUX 12.2	

	• DEBIAN GNU/LINUX 6.0.5 • UBUNTU 10.04 LTS • UBUNTU 12.04 LTS O CARACTERÍSTICAS: ▯ DEBE PROPORCIONAR LAS SIGUIENTES PROTECCIONES: • ANTIVIRUS DE ARCHIVOS RESIDENTE (ANTISPYWARE, ANTITROYANO, ANTIMALWARE, ETC.) QUE VERIFIQUE CUALQUIER ARCHIVO CREADO, ACCEDIDO O MODIFICADO; • LAS VACUNAS DEBEN SER ACTUALIZADAS POR EL FABRICANTE, COMO MÁXIMO, CADA HORA. ▯ CAPACIDAD DE CONFIGURAR EL PERMISO DE ACCESO A LAS FUNCIONES DEL ANTIVIRUS CON, COMO MÍNIMO, OPCIONES PARA LAS SIGUIENTES FUNCIONES: • GERENCIAMIENTO DE ESTATUS DE TAREAS (INICIAR, PAUSAR, PARAR O REANUDAR TAREAS); • GERENCIAMIENTO DE RESPALDO: CREACIÓN DE COPIAS DE LOS OBJETOS INFECTADOS EN UN RESERVORIO DE RESPALDO ANTES DEL INTENTO DE DESINFECTAR O ELIMINAR TAL OBJETO, SIENDO DE ESTA MANERA POSIBLE LA RESTAURACIÓN DE OBJETOS QUE CONTENGAN INFORMACIONES IMPORTANTES; • GERENCIAMIENTO DE CUARENTENA: CUARENTENA DE OBJETOS SOSPECHOSOS Y CORROMPIDOS, SALVANDO ESTOS ARCHIVOS EN UNA CARPETA DE CUARENTENA; • VERIFICACIÓN POR AGENDAMIENTO: BÚSQUEDA DE ARCHIVOS INFECTADOS Y SOSPECHOSOS (INCLUYENDO ARCHIVOS DENTRO DE UN RANGO ESPECIFICADO); ANÁLISIS DE ARCHIVOS; DESINFECCIÓN O ELIMINACIÓN DE OBJETOS INFECTADOS. ▯ EN CASO DE ERRORES, DEBE TENER CAPACIDAD DE CREAR LOGS AUTOMÁTICAMENTE, SIN	

	NECESIDAD DE OTROS SOFTWARE; ▯ CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS EN CASO DE QUE OTROS APLICATIVOS NECESITEN MÁS RECURSOS DE MEMORIA O PROCESAMIENTO; ▯ CAPACIDAD DE VERIFICAR ARCHIVOS POR CONTENIDO, O SEA, ÚNICAMENTE VERIFICARÁ EL ARCHIVO SI ES PASIBLE DE INFECCIÓN. EL ANTIVIRUS DEBE ANALIZAR LA INFORMACIÓN DE ENCABEZADO DEL ARCHIVO PARA TOMAR O NO ESA DECISIÓN A PARTIR DE LA EXTENSIÓN DEL ARCHIVO; ▯ CAPACIDAD DE VERIFICAR OBJETOS USANDO HEURÍSTICA; ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE SE GUARDARÁN LOS RESPALDOS Y ARCHIVOS EN CUARENTENA ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE LOS ARCHIVOS RECUPERADOS DE RESPALDO Y LOS ARCHIVOS SE GRABARÁN ▯ DEBE TENER MÓDULO DE ADMINISTRACIÓN REMOTO A TRAVÉS DE HERRAMIENTA NATIVA O WEBMIN (HERRAMIENTA NATIVA GNU-LINUX). • SERVIDORES WINDOWS – O COMPATIBILIDAD: ▯ MICROSOFT WINDOWS SMALL BUSINESS SERVER 2011 ESSENTIALS/STANDARD X64 ▯ MICROSOFT WINDOWS SERVER 2003 STANDARD/ENTERPRISE SP2 X86/X64 ▯ MICROSOFT WINDOWS SERVER 2003 R2 STANDARD/ENTERPRISE SP2 X86/X64 ▯ MICROSOFT WINDOWS SERVER 2008 STANDARD/ENTERPRISE/DATACENTER SP1 X86/X64 ▯ MICROSOFT WINDOWS SERVER 2008 CORE STANDARD/ENTERPRISE/DATACENTER SP1 X86/X64 ▯ MICROSOFT WINDOWS SERVER 2008 R2 STANDARD/ENTERPRISE/DATACENTER SP1	

	▯ MICROSOFT WINDOWS SERVER 2008 R2 CORE STANDARD/ENTERPRISE/DATACENTER SP1 ▯ MICROSOFT WINDOWS SERVER 2012 FOUNDATION/ESSENTIALS/STANDARD X64 ▯ MICROSOFT WINDOWS SERVER 2012 R2 STANDARD X64 ▯ MICROSOFT WINDOWS HYPER-V SERVER 2008 R2 SP1 ▯ MICROSOFT WINDOWS HYPER-V SERVER 2012 ▯ MICROSOFT TERMINAL BASADO EN WINDOWS SERVER 2003 ▯ MICROSOFT TERMINAL BASADO EN WINDOWS SERVER 2008 ▯ MICROSOFT TERMINAL BASADO EN WINDOWS SERVER 2008 R2 ▯ CITRIX PRESENTATION SERVER 4.0 Y 4.5 ▯ CITRIX XENAPP 4.5, 5.0 Y 6.0 O CARACTERÍSTICAS: ▯ DEBE PROPORCIONAR LAS SIGUIENTES PROTECCIONES: • ANTIVIRUS DE ARCHIVOS RESIDENTE (ANTISPYWARE, ANTITROYANO, ANTIMALWARE, ETC.) QUE VERIFIQUE CUALQUIER ARCHIVO CREADO, ACCEDIDO O MODIFICADO; • AUTOPROTECCIÓN CONTRA ATAQUES A LOS SERVICIOS/PROCESOS DEL ANTIVIRUS • FIREWALL CON IDS • CONTROL DE VULNERABILIDADES DE WINDOWS Y DE LOS APLICATIVOS INSTALADOS ▯ CAPACIDAD DE ELEGIR DE QUÉ MÓDULOS SE INSTALARÁN, TANTO EN LA INSTALACIÓN LOCAL COMO EN LA INSTALACIÓN REMOTA; ▯ LAS VACUNAS DEBEN SER ACTUALIZADAS	

	POR EL FABRICANTE, COMO MÁXIMO, CADA HORA. ▯ CAPACIDAD DE CONFIGURAR EL PERMISO DE ACCESO A LAS FUNCIONES DEL ANTIVIRUS CON, COMO MÍNIMO, OPCIONES PARA LAS SIGUIENTES FUNCIONES: • GERENCIAMIENTO DE ESTATUS DE TAREAS (INICIAR, PAUSAR, PARAR O REANUDAR TAREAS); • GERENCIAMIENTO DE TAREA (CREAR O EXCLUIR TAREAS DE VERIFICACIÓN) • LECTURA DE CONFIGURACIONES • MODIFICACIÓN DE CONFIGURACIONES • GERENCIAMENTO DE RESPALDO Y CUARENTENA • VISUALIZACIÓN DE INFORMES • GERENCIAMIENTO DE INFORMES • GERENCIAMIENTO DE CLAVES DE LICENCIA • GERENCIAMIENTO DE PERMISOS (AGREGAR/EXCLUIR PERMISOS SUPERIORES) ▯ EL MÓDULO DE FIREWALL DEBE CONTENER, COMO MÍNIMO, DOS CONJUNTOS DE REGLAS: • FILTRADO DE PAQUETES: DONDE EL ADMINISTRADOR PODRÁ ELEGIR PUERTAS, PROTOCOLOS O DIRECCIONES DE CONEXIÓN QUE SERÁN BLOQUEADAS/PERMITIDAS; • FILTRADO POR APLICATIVO: DONDE EL ADMINISTRADOR PODRÁ ELEGIR CUÁL APLICATIVO, GRUPO DE APLICATIVO, FABRICANTE DE APLICATIVO, VERSIÓN DE APLICATIVO O NOMBRE DE APLICATIVO TENDRÁ ACCESO A LA RED, CON LA POSIBILIDAD DE ELEGIR QUÉ PUERTAS Y PROTOCOLOS PODRÁN SER UTILIZADOS. ▯ CAPACIDAD DE SELECCIONAR POR SEPARADO EL NÚMERO DE PROCESOS QUE EJECUTARÁN FUNCIONES DE BARRIDO EN TIEMPO REAL, EL NÚMERO DE PROCESOS QUE EJECUTARÁN EL BARRIDO BAJO DEMANDA Y EL NÚMERO MÁXIMO	

	DE PROCESOS QUE PUEDEN SER EJECUTADOS EN TOTAL. ▯ CAPACIDAD DE REANUDAR AUTOMÁTICAMENTE TAREAS DE VERIFICACIÓN QUE HAYAN SIDO DETENIDAS POR ANORMALIDADES (CORTE DE ENERGÍA, ERRORES, ETC.) ▯ CAPACIDAD DE AUTOMÁTICAMENTE PAUSAR Y NO INICIAR TAREAS AGENDADAS EN CASO DE QUE EL SERVIDOR ESTÉ FUNCIONANDO CON FUENTE ININTERRUMPIDA DE ENERGÍA (UNINTERRUPTIBLE POWER SUPPLY – UPS) ▯ EN CASO DE ERRORES, DEBE TENER CAPACIDAD DE CREAR LOGS Y TRACES AUTOMÁTICAMENTE, SIN NECESIDAD DE OTROS SOFTWARE; ▯ CAPACIDAD DE CONFIGURAR NIVELES DE VERIFICACIÓN DIFERENTES PARA CADA CARPETA, GRUPO DE CARPETAS O ARCHIVOS DEL SERVIDOR. ▯ CAPACIDAD DE BLOQUEAR ACCESO AL SERVIDOR DE MÁQUINAS INFECTADAS Y CUANDO UNA MÁQUINA INTENTA GRABAR UN ARCHIVO INFECTADO EN EL SERVIDOR. ▯ CAPACIDAD DE CREAR UNA LISTA DE MÁQUINAS QUE NUNCA SERÁN BLOQUEADAS AUNQUE SEAN INFECTADAS. ▯ CAPACIDAD DE DETECCIÓN DE PRESENCIA DE ANTIVIRUS DE OTRO FABRICANTE QUE PUEDA CAUSAR INCOMPATIBILIDAD, BLOQUEANDO LA INSTALACIÓN; ▯ CAPACIDAD DE AGREGAR CARPETAS/ARCHIVOS PARA UNA ZONA DE EXCLUSIÓN, CON EL FIN DE EXCLUIRLOS DE LA VERIFICACIÓN. CAPACIDAD, TAMBIÉN, DE AGREGAR OBJETOS A LA LISTA DE EXCLUSIÓN DE ACUERDO CON EL RESULTADO DEL ANTIVIRUS, (EJ.: "WIN32.TROJAN.BANKER") PARA QUE CUALQUIER OBJETO DETECTADO CON EL RESULTADO ELEGIDO SEA IGNORADO; ▯ CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS EN CASO DE QUE OTROS	

	APLICATIVOS NECESITEN MÁS RECURSOS DE MEMORIA O PROCESAMIENTO; ▯ CAPACIDAD DE VERIFICAR ARCHIVOS POR CONTENIDO, O SEA, ÚNICAMENTE VERIFICARÁ EL ARCHIVO SI ES PASIBLE DE INFECCIÓN. EL ANTIVIRUS DEBE ANALIZAR LA INFORMACIÓN DE ENCABEZADO DEL ARCHIVO PARA TOMAR O NO ESA DECISIÓN A PARTIR DE LA EXTENSIÓN DEL ARCHIVO; ▯ CAPACIDAD DE VERIFICAR SOLAMENTE ARCHIVOS NUEVOS Y MODIFICADOS; ▯ CAPACIDAD DE ELEGIR QUÉ TIPO DE OBJETO COMPUESTO SERÁ VERIFICADO (EJ.: ARCHIVOS COMPRIMIDOS, ARCHIVOS AUTODESCOMPRESORES, .PST, ARCHIVOS COMPACTADOS POR COMPACTADORES BINARIOS, ETC.) ▯ CAPACIDAD DE VERIFICAR OBJETOS USANDO HEURÍSTICA; ▯ CAPACIDAD DE CONFIGURAR DIFERENTES ACCIONES PARA DIFERENTES TIPOS DE AMENAZAS; ▯ CAPACIDAD DE AGENDAR UNA PAUSA EN LA VERIFICACIÓN; ▯ CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE LA VERIFICACIÓN CUANDO SE INICIE UN APLICATIVO; ▯ EL ANTIVIRUS DE ARCHIVOS, AL ENCONTRAR UN OBJETO POTENCIALMENTE PELIGROSO, DEBE: • PREGUNTAR QUÉ HACER, O; • BLOQUEAR EL ACCESO AL OBJETO; O BORRAR EL OBJETO O INTENTAR DESINFECTARLO (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA POR EL ADMINISTRADOR); O CASO POSITIVO DE DESINFECCIÓN: ▯ RESTAURAR EL OBJETO PARA USO; O CASO NEGATIVO DE DESINFECCIÓN: ▯ MOVER PARA CUARENTENA O BORRAR (DE ACUERDO CON LA CONFIGURACIÓN PREESTABLECIDA	

	POR EL ADMINISTRADOR); ▯ ANTERIORMENTE A CUALQUIER INTENTO DE DESINFECCIÓN O EXCLUSIÓN PERMANENTE, EL ANTIVIRUS DEBE REALIZAR UN RESPALDO DEL OBJETO. ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE SE GUARDARÁN LOS RESPALDOS Y ARCHIVOS EN CUARENTENA ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE LOS ARCHIVOS RECUPERADOS DE RESPALDO Y LOS ARCHIVOS SE GRABARÁN ▯ DEBE CONTAR CON MÓDULO QUE ANALICE CADA SCRIPT EJECUTADO, BUSCANDO SEÑALES DE ACTIVIDAD MALICIOSA. • SERVIDORES LINUX – O COMPATIBILIDAD (O SUPERIOR): ▯ PLATAFORMA 32-BITS: • CANAIMA 3 • ASIANUX SERVER 3 SP4 • ASIANUX SERVER 4 SP1 • RED HAT ENTERPRISE LINUX 6.2 SERVER; • RED HAT ENTERPRISE LINUX 5.8 SERVER • FEDORA 16; • CENTOS-6.X (6.0-6.6) • SUSE LINUX ENTERPRISE SERVER 11 SP2; • NOVELL OPEN ENTERPRISE SERVER 11; • OPENSUSE LINUX 12.1; • OPENSUSE LINUX 12.2; • MANDRIVA ENTERPRISE SERVER 5.2; • UBUNTU SERVER 10.04.2 LTS;	

	• UBUNTU SERVER 12.04 LTS; • DEBIAN GNU/LINUX 6.0.5; • FREEBSD 8.3; • FREEBSD 9. ▯ PLATAFORMA 64-BITS: • CANAIMA 3 • ASIANUX SERVER 3 SP4 • ASIANUX SERVER 4 SP1 • RED HAT ENTERPRISE LINUX 6.2 SERVER; • RED HAT ENTERPRISE LINUX 5.8 SERVER • FEDORA 16; • CENTOS-6.2 • SUSE LINUX ENTERPRISE SERVER 11 SP2; • NOVELL OPEN ENTERPRISE SERVER 11; • OPENSUSE LINUX 12.1; • OPENSUSE LINUX 12.2; • MANDRIVA ENTERPRISE SERVER 5.2; • UBUNTU SERVER 10.04.2 LTS; • UBUNTU SERVER 12.04 LTS; • DEBIAN GNU/LINUX 6.0.5; • FREEBSD 8.3; • FREEBSD 9. O CARACTERÍSTICAS: ▯ DEBE PROPORCIONAR LAS SIGUIENTES PROTECCIONES: • ANTIVIRUS DE ARCHIVOS RESIDENTE (ANTISPYWARE, ANTITROYANO, ANTIMALWARE, ETC.)	

	QUE VERIFIQUE CUALQUIER ARCHIVO CREADO, ACCEDIDO O MODIFICADO; • LAS VACUNAS DEBEN SER ACTUALIZADAS POR EL FABRICANTE, COMO MÁXIMO, CADA HORA. ▯ CAPACIDAD DE CONFIGURAR EL PERMISO DE ACCESO A LAS FUNCIONES DEL ANTIVIRUS CON, COMO MÍNIMO, OPCIONES PARA LAS SIGUIENTES FUNCIONES: • GERENCIAMIENTO DE ESTATUS DE TAREAS (INICIAR, PAUSAR, PARAR O REANUDAR TAREAS); • GERENCIAMIENTO DE RESPALDO: CREACIÓN DE COPIAS DE LOS OBJETOS INFECTADOS EN UN RESERVORIO DE RESPALDO ANTES DEL INTENTO DE DESINFECTAR O ELIMINAR TAL OBJETO, SIENDO DE ESTA MANERA POSIBLE LA RESTAURACIÓN DE OBJETOS QUE CONTENGAN INFORMACIONES IMPORTANTES; • GERENCIAMIENTO DE CUARENTENA: CUARENTENA DE OBJETOS SOSPECHOSOS Y CORROMPIDOS, SALVANDO ESTOS ARCHIVOS EN UNA CARPETA DE CUARENTENA; • VERIFICACIÓN POR AGENDAMIENTO: BÚSQUEDA DE ARCHIVOS INFECTADOS Y SOSPECHOSOS (INCLUYENDO ARCHIVOS DENTRO DE UN RANGO ESPECIFICADO); ANÁLISIS DE ARCHIVOS; DESINFECCIÓN O ELIMINACIÓN DE OBJETOS INFECTADOS. ▯ EN CASO DE ERRORES, DEBE TENER CAPACIDAD DE CREAR LOGS AUTOMÁTICAMENTE, SIN NECESIDAD DE OTROS SOFTWARE; ▯ CAPACIDAD DE PAUSAR AUTOMÁTICAMENTE BARRIDOS AGENDADOS EN CASO DE QUE OTROS APLICATIVOS NECESITEN MÁS RECURSOS DE MEMORIA O PROCESAMIENTO; ▯ CAPACIDAD DE VERIFICAR ARCHIVOS POR CONTENIDO, O SEA, ÚNICAMENTE VERIFICARÁ EL ARCHIVO SI ES PASIBLE DE INFECCIÓN. EL ANTIVIRUS DEBE ANALIZAR LA INFORMACIÓN DE ENCABEZADO DEL ARCHIVO PARA TOMAR O NO ESA DECISIÓN A	

	PARTIR DE LA EXTENSIÓN DEL ARCHIVO; ▯ CAPACIDAD DE VERIFICAR OBJETOS USANDO HEURÍSTICA; ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE SE GUARDARÁN LOS RESPALDOS Y ARCHIVOS EN CUARENTENA ▯ POSIBILIDAD DE ELEGIR LA CARPETA DONDE LOS ARCHIVOS RECUPERADOS DE RESPALDO Y LOS ARCHIVOS SE GRABARÁN ▯ DEBE CONTAR CON MÓDULO DE ADMINISTRACIÓN REMOTO A TRAVÉS DE HERRAMIENTA NATIVA O WEBMIN (HERRAMIENTA NATIVA GNU-LINUX) • SERVIDORES NOVELL NETWARE: O COMPATIBILIDAD: ▯ NOVELL NETWARE 5.X SUPPORT PACK 6 O SUPERIOR ▯ NOVELL NETWARE 6.0 SUPPORT PACK 3 O SUPERIOR ▯ NOVELL NETWARE 6.5 SUPPORT PACK 3 O SUPERIOR O CARACTERÍSTICAS: ▯ DEBE CONTAR CON PROTECCIÓN EN TIEMPO REAL PARA ARCHIVOS ACCEDIDOS, CREADOS O MODIFICADOS; ▯ DEBE CONTAR CON VERIFICACIÓN MANUAL Y AGENDADA DE ACUERDO CON LA CONFIGURACIÓN DEL ADMINISTRADOR; ▯ CAPACIDAD DE REALIZAR ACTUALIZACIONES DE MANERA AUTOMÁTICA, VÍA INTERNET O LAN; ▯ CAPACIDAD DE HACER UN ROLLBACK DE LAS VACUNAS; ▯ CAPACIDAD DE MOVER ARCHIVOS SOSPECHOSOS O INFECTADOS AL ÁREA DE CUARENTENA;	

	▯ CAPACIDAD DE CREAR LOGS DETALLADOS Y GUARDAR RESULTADOS DE LAS VERIFICACIONES AGENDADAS; ▯ CAPACIDAD DE GUARDAR UN RESPALDO DE TODOS LOS OBJETOS INFECTADOS Y SOSPECHOSOS TRATADOS; ▯ CAPACIDAD DE NOTIFICAR AL ADMINISTRADOR DE BARRIDOS CONCLUIDOS Y SOBRE OBJETOS MALICIOSOS ENCONTRADOS EN EL SERVIDOR, UTILIZANDO LA RED NOVELL O CORREO ELECTRÓNICO; • SMARTPHONES Y TABLETS- O COMPATIBILIDAD: ▯ APPLE IOS 7.0 – 8.1 ▯ WINDOWS PHONE 8.1 ▯ ANDROID OS 2.3 - 5 O CARACTERÍSTICAS: ▯ DEBE PROPORCIONAR LAS SIGUIENTES PROTECCIONES PARA ANDROID: • PROTECCIÓN EN TIEMPO REAL DEL SISTEMA DE ARCHIVOS DEL DISPOSITIVO — INTERCEPTACIÓN Y VERIFICACIÓN DE: O TODOS LOS OBJETOS TRASMITIDOS USANDO CONEXIONES WIRELESS (PUERTA DE INFRARROJO, BLUETOOTH) Y MENSAJES EMS, DURANTE SINCRONISMO CON PC Y AL REALIZAR DESCARGAS USANDO EL BROWSER. O ARCHIVOS ABIERTOS EN EL SMARTPHONE O PROGRAMAS INSTALADOS USANDO LA INTERFACE DEL SMARTPHONE • VERIFICACIÓN DE LOS OBJETOS EN LA MEMORIA INTERNA DEL SMARTPHONE Y EN LAS TARJETAS DE EXPANSIÓN POR DEMANDA DEL USUARIO Y DE ACUERDO CON UN AGENDAMIENTO; ▯ DEBERÁ AISLAR EN ÁREA DE CUARENTENA	

	LOS ARCHIVOS INFECTADOS; ▯ DEBERÁ ACTUALIZAR LAS BASES DE VACUNAS DE MODO AGENDADO; ▯ DEBERÁ BLOQUEAR SPAMS DE SMS A TRAVÉS DE BLACK LISTS (LISTAS NEGRAS); ▯ DEBERÁ TENER FUNCIÓN DE BLOQUEO DEL APARATO EN CASO DE QUE LA SIM CARD SEA CAMBIADA POR OTRA NO AUTORIZADA; ▯ DEBERÁ TENER FUNCIÓN DE LIMPIEZA DE DATOS PERSONALES A DISTANCIA, EN CASO DE ROBO, POR EJEMPLO. ▯ DEBERÁ TENER FIREWALL PERSONAL; ▯ CAPACIDAD DE DETECTAR JAILBREAK EN DISPOSITIVOS IOS ▯ CAPACIDAD DE BLOQUEAR EL ACCESO A SITIOS POR CATEGORÍA EN DISPOSITIVOS ▯ CAPACIDAD DE BLOQUEAR EL ACCESO A SITIOS PHISHING O MALICIOSOS ▯ CAPACIDAD DE CREAR CONTENEDORES DE APLICATIVOS, SEPARANDO DATOS CORPORATIVOS DE DATOS PERSONALES ▯ CAPACIDAD DE CONFIGURAR WHITE Y BLACK LIST (LISTAS BLANCAS Y LISTAS NEGRAS) DE APLICATIVOS ▯ NAVEGADOR SEGURO PARA ANDROID Y PARA WINDOWS PHONE • MANEJO DE DISPOSITIVOS MÓVILES (MDM): O COMPATIBILIDAD: ▯ DISPOSITIVOS CONECTADOS A TRAVÉS DEL MICROSOFT EXCHANGE ACTIVESYNC • APPLE IOS • SYMBIAN OS • WINDOWS MOBILE Y WINDOWS PHONE	

	• ANDROID • PALM WEBOS ▯ DISPOSITIVOS CON SOPORTE AL APPLE PUSH NOTIFICATION (APNS) SERVICE • APPLE IOS 3.0 O SUPERIOR O CARACTERÍSTICAS: ▯ CAPACIDAD DE APLICAR POLÍTICAS DE ACTIVESYNC A TRAVÉS DEL SERVIDOR MICROSOFT EXCHANGE ▯ CAPACIDAD DE AJUSTAR LAS CONFIGURACIONES DE: • SINCRONIZACIÓN DE CORREO ELECTRÓNICO • USO DE APLICATIVOS • CONTRASEÑA DEL USUARIO • CIFRADO DE DATOS • CONEXIÓN DE MEDIOS EXTRAÍBLE ▯ CAPACIDAD DE INSTALAR CERTIFICADOS DIGITALES EN DISPOSITIVOS MÓVILES. ▯ CAPACIDAD DE, REMOTAMENTE, RESETEAR LA CONTRASEÑA DE DISPOSITIVOS IOS ▯ CAPACIDAD DE, REMOTAMENTE, BORRAR TODOS LOS DATOS DE DISPOSITIVOS IOS ▯ CAPACIDAD DE, REMOTAMENTE, BLOQUEAR UN DISPOSITIVO IOS	
Garantía y Soporte:	Certificación de la legalidad de las Licencias a nombre de Transcaribe S.A. El tiempo de derecho de actualización debe ser de tres (3) años, a partir de la entrega del producto.	CUMPLE
Instalación:	Las licencias deben tener respaldo directo del fabricante.	CUMPLE

CONCLUSIÓN:

La propuesta presentada por ACCESAR S.A.S., **CUMPLE** con los requisitos habilitantes técnicos exigidos en la invitación pública.

Una vez realizada la verificación de los documentos de habilitación de contenido jurídico, de experiencia y técnicos del proponente ACCESAR S.A.S., y valor económico, dentro del presente proceso, se concluye que la misma cumple con los requerimientos establecidos y por lo tanto los miembros del comité jurídico, técnico y financiero recomienda al ordenador del gasto, la adjudicación del proceso por valor de NUEVE MILLONES QUINIENTOS SETENTA Y NUEVE MIL CIENTO SESENTA Y CUATRO PESOS MCTE ($9.579.164). IVA Incluido.

Para constancia se firma en Cartagena de Indias D.T. y C., a los veintidós (22) días del mes de Diciembre de 2015

ERCILIA BARRIOS FLOREZ
Jefe Oficina Jurídica

JAIME JIMENEZ GONZALEZ
P.E Tesorero

MARIA ALEJANDRA FERREIRA H.
Asesor Jurídico Externo.

GERARDO MARRIAGA TOVAR
Profesional Especializado.