TDR

Adquisición e instalación de Software de Protección, Detección, Respuesta avanzadas y automatizadas de EndPoint (EDR).

DESCRIPCIÓN DE LA ADQUISICION:

Solución de Seguridad avanzada (para 1 año) son servidores y centros de datos, es un Software de implementación cliente – servidor con administración en premisa y opción de administración SaaS, Soporte de distintas versiones de Sistemas Operativos: Microsoft Windows, Linux, AIX, Docker.

Esto es una solución de seguridad avanzada que nos va a garantizar la seguridad, integridad y disponibilidad de la infraestructura de los servidores ante los ataques de día cero.

Esta solución permite un monitoreo constante de las maquinas virtuales (servicios simplificados), analizando el comportamiento de las actividades que se ejecutan, protegiéndonos de comportamiento y/o patrones maliciosos

Seguridad avanzada:

- Software de implementación cliente – servidor con administración en premisa y opción de administración SaaS, Soporte de distintas versiones de Sistemas Operativos: Microsoft Windows, Linux, AIX, Docker.
- Soporte de Implementación sobre ambientes virtuales: VMware NSX-T / NSX-V, Soporte de distintas plataformas cloud: AWS, Azure, Google.
- Protección avanzada de Antimalware con detección de comportamientos, reputación de archivos y web; correlación de EDR.
- Firewall e IPS para blindar Comunicaciones, puertos y protocolos y proteger contra ataques sobre vulnerabilidades y ataques de día cero en Sistemas operativos y aplicaciones.
- Monitoreo de integridad e inspección de eventos con control de aplicaciones para dar visibilidad sobre cualquier acción sobre archivos y rutas críticas, eventos relevantes para retroalimentar un SIEM y controlar la ejecución de aplicaciones no permitidas en los servidores.
- Capacidad Multi-Tenant que permita administrar distintas cuentas y servidores con capacidades de Seguridad y políticas de acuerdo a la necesidad de cada tenant.
- Incluir implementación de la solución (Llave en mano), incluyendo la creación del esquema multi-tenants y Entrenamiento de certificación para 7 empleados.

- La solución deberá permitir desde la misma consola la administración de los componentes: firewall, la prevención de Intrusos, antimalware, control de aplicaciones, monitoreo de integridad, la inspección de bitácoras y EDR
- Debe contar con capacidades de API que incluye un SDK de Python
- La solución deberá ser administrada por consola web
- La solución debe ser en premisa para su funcionamiento con opcion a licenciarlo SaaS.
- La consola de administración debe contar con Tableros o Dashboards que permitan monitorear los equipos de forma sencilla y estos pueden ser personalizados por el administrador.
- La solución deberá tener la capacidad de reconocer los agentes desplegados y hacer descubrimiento de equipos en la red y mediante integración de Vmware, vCloud, Google Cloud Platform, AWS y Azure.
- La solución deberá tener la capacidad de instalar agentes en los servidores a través de scripts, los cuales pueden ejecutarse de forma manual o calendarizada en servidores físicos, virtuales o de nube.
- La solución debe contar con la capacidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración.
- La solución debe incorporar la capacidad de integrase con la plataforma de EDR para reenvío de logs y también telemetría para su correlación
- La solución deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio.
- Debe soportar las siguientes bases de datos:
  PostgreSQL 13.x (only Core or Amazon RDS distributions)
  PostgreSQL 12.x (only Core or Amazon RDS distributions)
  PostgreSQL 11.x (only Core, Amazon RDS, or Amazon Aurora distributions)
  PostgreSQL 10.x (only Core, Amazon RDS, or Amazon Aurora distributions)
  PostgreSQL 9.6.x (only Core, Amazon RDS, or Amazon Aurora distributions)
  Microsoft SQL Server 2019
  Microsoft SQL Server 2017
  Microsoft SQL Server 2016
  Microsoft SQL Server 2014
  Microsoft SQL Server 2012
  Microsoft SQL RDS
  Oracle 11g, 12c, 18c, 19c, all supported when deployed as software or when used with Amazon RDS
  Oracle RAC12c Release 1 (v12.1.0.2.0) on SUSE Linux Enterprise Server 11 SP3

Oracle RAC 12c Release 1 (v12.1.0.2.0) on Red Hat Linux Enterprise Server 6.6
Oracle RAC 12c Release 1 (v12.1.0.2) on Red Hat Linux Enterprise Server 7.0

- La solución deberá contar con la capacidad de crear etiquetas para identificar y ordenar eventos importantes de seguridad, así como separarlos y crear paneles de seguridad e informes personalizados para aliviar la carga de la administración
- La solución debe contar con políticas por defecto que eviten la desinstalación del agente de seguridad y/o la baja de servicios del mismo. (Agent Self Protection)
- La solución deberá permitir la distribución de patrones, motores y nuevos componentes a través de agentes de actualización que pueden distribuirse en el ambiente.
- Los agentes de actualización deben buscar las actualizaciones de firmas y componentes y distribuirlas a los agentes, estas actualizaciones deben realizarse en modo seguro utilizando comunicación SSL con el servidor del cual se descarga dicha información.
- La solución debe permitir la creación de políticas globales para todas las maquinas, por perfil e individualmente para cada servidor.
- La solución debe contar con la capacidad de generar paquetes de auto-diagnostico que permita la recolección de archivos relevantes para envío al fabricante en caso de requerir soporte del producto.
- El agente de protección debe tener compatibilidad con los siguientes sistemas operativos: **Microsoft® Windows®:**
    - Windows Server 2022 (LTSC, version 21H2) (64-bit)
    - Windows Server 2019 (LTSC, version 1809) (64-bit)
    - **Windows Server Core (SAC, version 1709) (64-bit)**
    - Windows Server 2016 (LTSC, version 1607) (64-bit)
    - Windows Server 2012 R2 (64-bit)
    - Windows Server 2012 (64-bit)
    - Windows Server 2008 R2 (64-bit)
    - Windows Server 2008 (32/64-bit)
    - Windows Server 2003 R2 SP2 (32/64-bit)
    - Windows Server 2003 SP1 o SP2 (32/64-bit)
    - Windows 2000 Service Pack 3 o 4 (32-bit)
    - Windows 11 (64-bit)
    - Windows 10 Embedded (64-bit)
    - Windows 10 (32/64-bit)
    - Windows 8.1 Embedded (32-bit)
    - Windows 8.1 (32/64-bit)
    - Windows 8 (32/64-bit)
    - Windows 7 (32/64-bit)
    - Windows 7 Embedded (32-bit)

- Windows XP (32/64-bit)

Linux:

- Red Hat Enterprise Linux 5 (32/64-bit)
- Red Hat Enterprise Linux 6 (32/64-bit)
- Red Hat Enterprise Linux 7 (64-bit)
- Red Hat Enterprise Linux 8 (64-bit)
- Red Hat Enterprise Linux 8 (AWS ARM-Based Graviton 2)
- Ubuntu 10 (64-bit)
- Ubuntu 12 (64-bit)
- Ubuntu 14 (64-bit)
- Ubuntu 16 (64-bit)
- Ubuntu 18 (64-bit)
- Ubuntu 20.04 (64-bit)
- CentOS 5 (32/64-bit)
- CentOS 6 (32/64-bit)
- CentOS 7 (64-bit)
- CentOS 8 (64-bit)
- Rocky Linux 8 (64-bit)
- Debian 6 (64-bit)
- Debian 7 (64-bit)
- Debian 8 (64-bit)
- Debian 9 (64-bit)
- Debian 10 (64-bit)
- Debian 11 (64-bit)
- Amazon Linux (64-bit)
- Amazon Linux 2 (64-bit)
- Amazon Linux 2 (64-bit Arm)
- Oracle Linux 5 (32/64-bit)
- Oracle Linux 6 (32/64-bit)
- Oracle Linux 7 (64-bit)
- Oracle Linux 8 (64-bit)
- SUSE Linux Enterprise Server 11 (32/64-bit)
- SUSE Linux Enterprise Server 12 (64-bit)
- SUSE Linux Enterprise Server 15 (64-bit)
- CloudLinux 5 (32/64-bit)
- CloudLinux 6 (32-bit)
- CloudLinux 6 (64-bit)
- CloudLinux 7 (64-bit)
- CloudLinux 8 (64-bit)
- AlmaLinux 8 (64-bit)

- Solaris 10 Updates 4-6 (64-bit, SPARC or x86)
- Solaris 10 Updates 7-10 (64-bit, SPARC or x86)
- Solaris 10 Update 11 (64-bit, SPARC or x86)
- Solaris 11.0 (1111)-11.1 (64-bit, SPARC or x86)
- Solaris 11.2-11.3 (64-bit, SPARC or x86)
- Solaris 11.4 (64-bit, SPARC or x86)
- AIX 6.1, 7.1, 7.2
- Vmware
- VMware vCenter 6.7 with ESXi 6.7
- VMware vCenter 6.5 with ESXi 6.0 or 6.5
- VMware vCenter 6.0 with ESXi 6.0
- VMware Tools on each ESXi host (including Guest Introspection)
- VMware NSX Manager 6.3 or later
- VMware vSphere 6.5 con NSX para vSphere 6.3.0.
- VMware NSX-T / NSX-V
- Docker
- Docker v1.12.x, v1.13.x

Docker CE

- 17.03
- 17.09
- 17.12
- 18.03
- 18.06
- 18.09
- 19.03

Docker EE

- 17.06
- 18.03
- 18.06
- 18.09
- 19.03

- La solución deberá contener un firewall que proteja servidores físicos y/o virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros: Protocolos: ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP. Direcciones MAC. Direcciones IP. Puertos TCP & UDP.

- Garantía / Contrato por 1 año y Licencias no pueden ser en la nube, deben ser en las premisas del cliente (licencia perpetua).

FIREWALL Y REPUTACIÓN WEB

- La solución deberá ser capaz de hacer un escaneo de puertos en los servidores protegidos para identificar puertos utilizados con el objetivo de personalizar las políticas.
- La solución deberá ser capaz de configurar la prioridad de la tarjeta de red cuando el servidor tenga múltiples tarjetas de conexión.
- La solución deberá ser capaz de detectar comportamientos correspondientes a descubrimientos, es decir, en donde el atacante busca mapear la red. Al detectar este tipo de escaneo debe poder bloquear todo tráfico de ese host malicioso hasta por 30 minutos.
- La solución permitirá monitorear el tráfico para registrar algún ataque y bloquear el tráfico relacionado con él sin afectar el tráfico normal no relacionado con el ataque, permitiendo que continúen disponibles los servicios del servidor.
- El modulo de Firewall debe permitir trabajar en modo TAP para pruebas e Inline para bloqueo.
- El firewall debe permitir la creación de reglas por protocolo, origen del tráfico, frame type, cabeceras TCP y destino del tráfico.
- Las reglas del firewall deben permitir las siguientes acciones: Allow, Log Only, Bypass, Force Allow y Deny.
- La solución debe contar con mecanismo de control y seguimiento de sesión (stateful) para el protocolo UDP.
- La solución contara con la capacidad de limitar el número de conexiones entrantes y salientes de un equipo determinado.
- La solución debe ofrecer una amplia cobertura para todos los protocolos basados en IP y tipos de tramas así como un filtrado preciso para puertos y direcciones IP y MAC.
- La solución deberá tener la capacidad de bloquear el tráfico entre las tarjetas de red de los servidores.
- El módulo de Firewall debe ser capaz de configurarse en modo Fail Open o Fail Closed
- El Firewall debe poder trabajar en modo Stateful y debe ser configurable
- El módulo de protección del Firewall de host debe contar con la posibilidad de aplicar las políticas de manera programada sobre ciertos horarios.
- La reputación Web debe incluir en la integración con los servicios de reputación (del mismo fabricante) para mejorar la protección contra amenazas, incluyendo servicio de reputación de archivo y reputación de URLs

- La funcionalidad de reputación de URLs debe evitar la conexión a sitios de mala reputación que puedan poner en riesgo la información que reside en los servidores.
- El módulo de reputación web debe permitir configurar los puertos a inspeccionar, permitiendo usar puertos puntuales o listas de puertos sobre los cuales verificar las comunicaciones. Debe permitir escanear contra los 65535 puertos
- La reputación Web debe poder configurarse en 3 niveles: High/Medium/Low
- El módulo de reputación Web debe poder detectar y bloquear comunicaciones de Comando y Control hacia IPs, Dominios y URLs
- La solución deberá proteger aquellas vulnerabilidades recientemente descubiertas, aplicando la protección en los servidores sin tener que reiniciar el sistema o modificar el código fuente de la aplicación o sistema operativo.
- La solución deberá incluir protección inmediata de vulnerabilidades para más de 100 aplicaciones y sistemas operativos, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP entre otras.
- La solución debe proteger ataques de tipo Inyección de SQL, secuencias de comandos de sitios cruzados (Cross- Site Scripting) y otras vulnerabilidades de las aplicaciones web.
- La solución deberá proteger las brechas de seguridad de forma automática y transparente, interrumpiendo únicamente el tráfico malicioso.
- La solución deberá contar con un módulo que permita, de forma automatizada, la protección de las vulnerabilidades de software que se hayan detectado en la fase de escaneo mediante tecnología de blindaje, sin la necesidad de implementar parches de sistema operativo o actualizaciones en los aplicaciones instaladas.
- El blindaje deberá realizarse sin la necesidad de aplicar reglas o configuraciones manuales, garantizando la entera automatización del proceso.
- La solución deberá cubrir vulnerabilidades de sistemas operativos Windows 2000, 2003 server y 2008 server independientemente de que Microsoft ya no genere parches de seguridad para mantener los niveles de protección.
- La solución deberá realizar escaneos en los servidores y determinar automáticamente los parches virtuales o reglas de blindaje que se requieren aplicar para proteger las vulnerabilidades del sistema operativo y aplicaciones que se encuentran corriendo sobre dichos servidores.
- La solución deberá ser capaz de detectar y prevenir actividad de conexiones de C&C asociadas a ransomware a través de la red, mediante la inspección del tráfico para identificar técnicas de comunicación conocidas utilizadas en ataques de ransomware.
- Capacidad de bloquear el tráfico entre las tarjetas de red de los servidores.
- El IPS debe ser capaz de Reemplazar secuencia de bytes sospechosas y sanitizar la comunicación

- El IPS debe poder hacer drop a paquetes maliciosos
- El IPS debe poder hacer un Reset a comunicaciones maliciosas
- El IPS debe contar on un escaneo de recomendaciones que asigna automáticamente las reglas necesarias a un servidor para proteger vulnerabilidades en producción sin necesidad de reinicio.
- El módulo de IPS debe poder inspeccionar tráfico SSL/TLS
- El módulo de IPS debe poder configurarse en modo de prevención o detección.

ANTIMALWARE

- Debe permitir configurar AMSI y debe venir habilitado por defecto
- Debe escanear procesos corriendo, y en caso de encontrar uno malicioso debe poder terminarlo.
- La solución deberá realizar escaneos en tiempo real. los escaneos programados y los escaneos bajo demanda deben contar con la posibilidad de manejar excepciones en función de: tipos de archivos y rutas
- La solución debe ofrecer la opción de elegir que se ejecute una acción automática en función de la amenaza detectada.
- La solución debe contar con la capacidad de limpieza, borrado y envío a cuarentena del archivo detectado como amenaza.
- La solución debe contar con caché para los escaneos en tiempo real y programados, con el objetivo de optimizar el consumo de recursos en los servidores virtuales.
- La solución deberá contar con un módulo de protección basado en análisis de comportamiento para protección contra amenazas desconocidas o nuevas variantes, detectando y controlando comportamientos no autorizados u anómalos.
- La solución Deberá contar con protección contra ransomware sin depender de que la firma de la amenaza sea detectada por patrón, detectando comportamientos de cifrado o modificación de archivos no autorizados y que permita recuperar el archivo original en caso de que dicho archivo haya sido cifrado.
- La solución deberá ser capaz de proteger los documentos contra cifrados o modificaciones no autorizadas, además de tener la capacidad, de poder crear copias de archivos cifrados, dando oportunidad a los usuarios de recuperar los archivos que pueden haber sido cifrados por un proceso de ransomware
- La solución deberá levantar un listado de objetos sospechosos para retroalimentar sandbox externo para análisis de amenazas desconocidas.

MONITOREO DE INTEGRIDAD

- Debe poder alertar de cambios no esperados sobre llaves de registro, servicios, procesos, software instalado, puertos y archivos.
- La solución deberá inspeccionar las bitácoras del sistema para identificar eventos de seguridad en los servidores y recomendar automáticamente reglas en base al sistema operativo y aplicaciones instaladas en cada uno de los servidores.

- La solución deberá contar con alertas en tiempo real cuando un evento crítico o relevante sea generado, o cuando se detecte una modificación en carpetas, archivos o llaves de registro del sistema operativo y aplicaciones.
- La solución debe ofrecer un escaneo que identifique recomendaciones de proceso y servicios que se estén ejecutando para aplicar las reglas de monitoreo.
- La solución debe identificar y ejecutar automáticamente reglas de monitoreo de integridad, para realizar el monitoreo de cambios del sistema operativo y las aplicaciones instaladas en el servidor.
- La solución debe identificar y ejecutar automáticamente reglas de monitoreo de integridad, para realizar el monitoreo de cambios del sistema operativo y las aplicaciones instaladas en el servidor.
- La solución debe contar con la Capacidad de ejecutar tareas programadas y asignar de manera automatizada las reglas de monitoreo de integridad y de bitácoras recomendadas por la propia solución con el fin de mantener la protección integral de los servidores.

INSPECCIÓN DE LOGS

- Debe poder capturar y dar correlación de eventos en el server con posibles ataques
- La solución debe brindar alertas sobre los eventos de seguridad, deberá ser enviado a sistemas de correlación (SIEM) vía protocolos o métodos estándares, como Syslog, SNMP y/o correo electrónico.
- La solución debe inspeccionar bitácoras de sistema operativo y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos.
- Capacidad de crear reglas personalizadas para el monitoreo de bitácoras.
- La solución debe tener la capacidad de inspeccionar eventos generados:
- En el visor de eventos para los servidores de plataformas Windows.
- En el “syslog messages” de servidores con sistema operativo Linux.
- La solución se puede integrar con herramientas como ArcSight, NetlQ, Intellitactics, RSA Envision, Q1Labs, Loglogic, Sentinel.

CONTROL DE APLICACIONES

- Debe realizar un inventario de elementos ejecutables en el servidor para posteriormente bloquear o permitir software en función de la configuración.
- La solución debe detectar y bloquear software no autorizado automáticamente
- La plataforma deberá realizar escaneos de equipos y determinar aplicaciones que se encuentran instaladas en ese momento.
- La plataforma deberá evitar la ejecución de nuevas aplicaciones que no estén permitidas.
- La plataforma deberá detener amenazas que no tienen firma, incluyendo algunas amenazas zero-day.
- La plataforma deberá poder determinar si en el inventario de software de los servidores hay software nuevo o si ha cambiado, la solución debe comparar los

archivos con los valores hash del software inicialmente instalado. El cambio incluye diferencias en: Nombre del archivo, Ruta o ubicación, Marca de tiempo, Permisos, Contenido del archivo.

- Cuando el control de aplicaciones encuentra un nuevo software, debera decidir si lo permite o lo bloquea. Para decidir, el control de la aplicación compara el archivo del software: Hash, Tamaño del archivo, Path, Nombre del Archivo.
- El control de la aplicación podrá realizar búsquedas en los archivos de software cuando se examina la instalación inicial y se monitorea el cambio. El software auditado podrá ser: Sistema operativo, bibliotecas de linux y otros binarios y bibliotecas, Archivos Java, .jar y . class (y otros codigos de bytes compilados), Scripts de PHP, Python y Shell (y otras aplicaciones web y scripts que se interpretan o compilan sobre la marcha).

EDR

- La plataforma de EDR debe cumplir con los estandares de ISO 27001, ISO 27014, ISO 27034-1, ISO 27017, SOC2.
- El EDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.
- Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.
- La Plataforma de EDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.
- Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.
- Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.
- Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).
- Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
- EDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.
- Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.
- Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.
- Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.

- Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.
- Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.
- Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico.
- Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor
- La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campaña asociada, la Plataforma atacada, inteligencia e indicadores
- Debe proveer enlaces desde el workbench a la documentación del framework de MITRE ATT&CK.
- En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.
- Debe ofrecer opciones de respuesta "context aware" para acciones rápida desde la plataforma.
- Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence.
- Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.
- Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud.

MULTI TENANT

- La solucion debe poder crear múltiples entornos de administración distintos utilizando una única base de datos.
- Aíslar completamente la configuración, las políticas, las computadoras y los eventos de cada inquilino o tenant.
- Debe brindar un administrador unico para cada inquilino o tenant.Debe proporcionar segmentación para las unidades de negocio dentro de una organización.
- Cada unidad de negocio debe ser un inquilino o tenant independiente
- Los inquilinos o tenants deben ser responsables de la creación y administración de sus propias computadoras, políticas, configuraciones y eventos. Independiente de cualquier otro inquilino y deben ser invisibles para otros inquilinos o tenants.
- La administracion de activación debe ser por medio de envio de correo SMTP.
- La consola de administracion Multi Tenant debe brindar visibilidad del uso de recursos de los inquilinos o tenant por medio de gráficos de facil lectura y tener la capacidad de generar reportes.

PLAZO DE EJECUCIÓN

Una vez seleccionado el proveedor de esta aplicación tenemos un plazo de 2 semanas para la implementación por el nivel de urgencia que se requiere.

CONDICIONES DE GARANTIA DEL SERVICIO

- Soporte de fabricante por 1 año.
- El proveedor debe instalar y garantizar la implementacion del servicio.

- Acceso permanente al Centro de asistencia técnica, soporte 24/7/365, además de acceso a la comunidad de la aplicación seleccionada, supervisada de forma activa por los especialistas. gestionar todos los recursos incluidos en la asistencia técnica básica y en la asistencia técnica por e-mail.