Requerimientos, Características

- Computador portátil (laptop)
  Procesador:
- Frecuencia de Reloj: 1.60 GHZ o superior
- Cuatro núcleos
- Equivalente a Atom y/o Celeron, o superior
  (Procesadores similares al Celeron Quad Core, Pentium Quead Core, Core i3 y AMD A8 Quad Core)
- 4 GB de memoria RAM como mínimo
- 500 GB en espacio de Disco Duro (en HDD), (128 GB si es en SSD) como mínimo
- Tarjeta de Red (Ethernet) de Area local (LAN) 10/100/1000 Mbps, Wi-Fi 802-.11 n/ac
- Tarjeta de Video
- Salida de video HDMI y VGA
- Tres (3) puertos USB 2.0 y Dos puertos 3.0 al menos
- Sistema Operativo: Windows 10 64 Bits o superior en español
- Monitor 15 – 17 pulgadas, LCD, Antirreflejo, Wide Screen
- Resolución 1440 x 900 o superior
- Teclado USB en Español
- Alimentación eléctrica de 19 voltios, 65 watts ac-dc con fuente y cables incluidos (tratar de que sea un equipo de bajo consumo).
- Software de ofimática: Microsoft Office 2016, 64 Bits.
- Solución de seguridad centralizada con licenciamiento a 2 años o más (ver especificaciones abajo).
- Constancia de que los equipos cumplen con las siguientes normas de calidad internacional (Ej: CE, FCC, UL, o CUL)
- 2 años de garantía en piezas y servicios como mínimo. El suplidor debe brindar un proceso para la reclamación y manejo de garantía con asistencia al usuario de manera local, y los contactos (teléfono, mail, web-side, etc.) debidamente informados por escrito adjunto al equipo.
- En el caso de la garantía, el reemplazo de equipos o partes defectuosas debe ser posible de llevarse a cabo en un margen no mayor de 30 días hábiles
- El suplidor de las laptops debe ser distribuidor autorizado de la marca y respaldar la garantía del fabricante.

Grabado de identificación del equipo

Cada laptop llevara un grabado de identificación de donación (logo del INDOTEL) detrás de la pantalla en la parte superior izquierda, mostrando que es un aporte de la institución.

Especificaciones grabado de identificación

- Dimensiones: 2 x 16 pulgadas (5.08 x 4.064 centímetros).
- Logo del INDOTEL colocado en la laptop detrás de la pantalla, en la parte superior izquierda
- Diseño: Sobre un material transparente para que solo se vea el logo y el borde sobre la maquina (opción 1) o diseño invertido que se puede hacer un troquel

para que la parte del logo se vea rellenada por la superficie del equipo (opción 2. El INDOTEL proporcionara el modelo, Ambos de un solo color.

Solución de seguridad centralizada para dispositivos finales

Se requiere de una solución de seguridad con controlador centralizado capaz de llevar a cabo las siguientes funciones:

- La solución propuesta debe permitir la gestión de seguridad a partir de un sistema centralizado de gerencia o de un firewall del mismo fabricante.
- La solución propuesta debe poder utilizar múltiples perfiles de configuración de acuerdo al segmento de red donde la misma se encuentre.
- La solución propuesta debe ser capaz de compartir telemetría de los dispositivos finales, para en base a la misma brindar conocimientos del estado actual de los equipos, y proveer obediencia y ejecución de las instrucciones de seguridad emitidas por el controlador en base a las políticas de la seguridad de la organización propietaria de la plataforma.
- La solución propuesta debe ser capaz de automatizar la prevención de amenazas conocidas y desconocidas a través de una plataforma de componentes de seguridad integrada en el dispositivo final y posible interrogación a un sandbox.
- La solución propuesta debe funcionar en modo "sandalone" sin necesidad de administración centralizada.
- La solución en modo "standalone" no debe requerir licenciamiento.
- La solución propuesta debe permitir hasta 10 clientes administrados de forma centralizada gratuitos para poder realizar la instalación de laboratorios interinos.
- La solución debe ser capaz de realizar un backup y restauración del archivo de configuración del cliente de seguridad.
- La solución debe ser capaz de poner en cuarentena los equipos finales en caso de ser necesario, desconectándolos de la red y prevenir la infección de los otros equipos.
- La solución propuesta debe der capaz de proveer acceso remoto seguro y de fácil uso a través de SSL e IPsec VPN.
- La solución propuesta debe ser capaz de verificar la postura de seguridad del dispositivo final.
- La solución propuesta deber capaz de someter a los dispositivos finales a obedecer los cumplimientos mínimos de vulnerabilidad y la versión del sistema.
- La solución propuesta debe ser capaz de detección de dispositivos autorizados.
- Los componentes de seguridad y de VPN que el dispositivo final del a solución de seguridad centralizada debe de poseer son:
    - Antivirus
    - Detección de sandbox
    - Filtrado Web
    - Firewall de aplicación
    - IPsec VPN
    - SSL VP
- La solución propuesta debe permitir la configuración de parámetros del sistema vía XML (eXtensible Markup Language)
- La solución propuesta debe permitir que durante la instalación se elija cuales componentes de la misma serán ejecutadas.

- El fabricante debe poseer portal para descargar el cliente de seguridad e instalación directa en los sistemas operativos.
- El sistema de gestión centralizada debe ser capaz de instalar el cliente de seguridad en equipos con sistema operativo Windows en un dominio de Windows.
- El cliente de la solución de seguridad para dispositivos finales debe de ser compatible con los siguientes sistemas operativos:
    - Windows 7
    - Windows 8
    - Windows 8.1
    - Windows 10
    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Mac OS X v10.8
    - Mac OS X v10.9
    - Mac OS X v10.10
    - Mac OS X v10.11
    - OIS 5.1 o superior
    - Android 4.4.4 o superior
- El suplidor de la solución de seguridad centralizada debe ser distribuidor autorizado de la marca y respaldar la garantía del fabricante.
- El controlador remoto de la solución de seguridad centralizada debe de ser compatible con los siguientes sistemas operativos

    - Windows 7
    - Windows 8
    - Windows 8.1
    - Windows 10
    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016

- La solución de seguridad centralizada debe soportar las siguientes opciones de autenticación:
    - RADIUS
    - LDAP
    - Base de datos locas
    - xAuth
    - TACACS+
    - Certificado digital (formato X509)

- La solución de seguridad centralizada debe soportar la siguientes opciones de conexión:
    - Auto conectar VPN antes del inicio de sesión del sistema operativo
    - Configuración del modo IKE para el túnel VPN IPsec.

- La solución de seguridad centralizada su controlador y la solución integrada en los dispositivos finales, debe de ofrecer licenciamiento por 1 año.
- La solución de seguridad centralizada debe de brindar ante para la plataforma de los dispositivos finales como para el controlador central soporte 24x7

Controlador centralizado de la Solución

Especificaciones Técnicas

- Procesador Xeon i7 quad core de 64 bit a 2.0 GHZ
- 16 Gb de RAM
- 1 TB de disco duro
- Adaptador Gigabit (10/100/1000BaseT) Ethernet de acceso a Internet.

El controlador centralizado de la solución de seguridad debe brindar:

- Interfaz de usuario simple y fácil de usar
- Debe poseer una interfaz de gestión vía navegador de red
- Gestión de los clientes localizados tanto en una red de área local como a través de internet
- Generación y envió de reportajes y registro de los componentes de seguridad a un analizador remoto del mismo fabricante
- Aprovisionamiento centralizado de los clientes
- Generación y envió de reportajes y registros de los componentes de seguridad a un analizador remoto del mismo fabricante.
- Despliegue remoto de la plataforma de seguridad de los dispositivos finales
- Ejecución de escaneos de antivirus y de vulnerabilidad en los dispositivos finales de forma controlada: diario, semanal, mensual, etc.
- El escaneo debe ser capaz de gestionar el tipo de barrido completo o parcial
- Ejecución de actualizaciones y parchado de vulnerabilidades detectadas en los dispositivos finales de forma controlada
- Clasificación de sitios web a través de comodines expresiones regulares y sus posibles acciones: bloquear o permitir
- Un dashboard en el sistema de gestión centralizada para proporcionar información sobre: Cantidad de dispositivos administrados, Versión del sistema operativo.

    - Cantidad de dispositivos administrados
    - Versión del sistema operativo
    - Perfil de instalación, Usuario
    - Versión de firma Antivirus
    - IP del cliente
    - Estado de seguridad del cliente
    - Estado de registro del cliente
    - Sistema operativo donde se está instalando el cliente de seguridad
    - Perfil de cliente de seguridad
    - Funciones de seguridad habilitadas en el cliente de seguridad
    - Vulnerabilidades detectadas

- Opción para que el usuario tenga acceso a la configuración del cliente de seguridad por contraseña solamente.
- Gestion de la instalación junto al sistema de gestión de forma silenciosa
- Integración de directorio activo, pudiendo utilizar las mismas unidades organizacionales de los miembros de una institucion para el manejo del dispositivo final.
- Alertas por correo electrónico automáticas.
- Soporte para grupos personalizados

- Disparadores Remotos
- Capacidad de realizar copias de seguridad dela base de datos
- Creación de usuarios con diferentes derechos de administración
- Configuración de los perfiles de los clientes de seguridad vía XML
  Importación de perfil de configuración de firewalls del mismo fabricante.
- Configuración de diferentes perfiles y diferentes grupos de clientes de seguridad para facilitar la gestión del conjunto de clientes de seguridad instalados.
- Creación de perfiles de cliente de seguridad incluyendo antivirus, filtro web, firewall de aplicación y red privada virtual (VPN)
- Integración con un firewall de la misma marca del fabricante para establecer reglas de obediencia.
- Licenciamiento basado en la cantidad de clientes que serán gestionados de forma centralizada.