ANEXO 1 TÉCNICO

Contratar la adquisición de 670 nuevas licencias de software antivirus con vigencia de un año para la ANI, Instalación, configuración, soporte, capacitación.

CONSOLA DE ADMINISTRACIÓN ALOJADA EN LA NUBE O LOCAL

La solución debe soportar una red con directorio activo y con integración a él.
La solución debe tener una gestión centralizada mediante una consola Cloud principal y posibilidad de tener varias consolas distribuidas.
La solución debe ser actualizada cuando haya nuevas actualizaciones del software y estas estén disponibles durante la vigencia del contrato.
La solución debe tener un impacto mínimo en el tráfico WAN y conexiones a sedes remotas.
La solución debe permitir la implementación de políticas por direccionamiento IP o aplicaciones.
La solución debe tener la capacidad de descubrir dispositivos físicos y virtuales.
La solución de antivirus debe soportar la instalación de los agentes en estaciones de trabajo, portátiles, servidores y opcionalmente en dispositivos móviles (Tabletas, teléfonos inteligentes).
Múltiples capas de Seguridad para puntos finales: antivirus y antimalware con monitorización del comportamiento
Protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas
La solución debe tener cortafuego, control de dispositivos y control de contenidos, con antiphising y antispam para servidores de correo
La solución de antivirus debe incluir filtrado web y seguridad web.
La solución debe permitir la distribución de firmas desde la consola central hacia todos los agentes.
La solución debe brindar la posibilidad de bloquear o restringir remotamente el acceso de los usuarios a ciertas aplicaciones y páginas Web
La solución debe ofrecer protección contra hacking, poshing y ransomware, con características de cortafuego, IDS y filtrado WEB
La solución debe permitir la distribución del agente en imágenes de OS pre empaquetadas.
La solución debe permitir la instalación del agente de manera stand-alone.
La solución debe permitir la creación de grupos de políticas para los agentes.
La solución debe permitir la instalación automática del agente sin intervención del administrador.
La solución debe contar con un módulo de corta fuegos Bidireccional (firewall) y poder trabajar en conjunto con el firewall propietario del sistema operativo en el cual está instalado el agente.
La solución debe permitir la desinstalación remota del agente.
La solución debe permitirle al administrador la instalación, configuración, reconfiguración, actualización o desinstalación de cualquier agente en mal funcionamiento.
La solución debe permitir el bloqueo de la opción de desinstalación de los agentes mediante contraseña u otro medio de gestión administrativa única.
La solución debe permitir opciones de escaneo liviano o a profundidad de los archivos del dispositivo escaneado.
La solución debe permitir la configuración de escaneos en uso liviano o extensivo de la CPU.

La consola central de administración de la solución debe permitir tener actualizada la información de manera precisa sobre la cantidad de dispositivos con el agente instalado la cantidad de dispositivos que no cuentan con el agente instalado.

La consola debe permitir el acceso a la gestión solo después de haberse autenticado con usuario y contraseña de directorio activo.

La consola debe permitir la creación de un usuario local que sea administrador de la maquina con todos los privilegios en caso de perder la conexión contra el directorio activo.

La consola de gestión deber permitir la creación de grupos o usuarios administradores e integrarse con el directorio activo.

La consola central de gestión debe permitir la configuración de repositorios de actualización de firmas distribuidos localmente en las instalaciones de la entidad.

La consola de gestión debe permitir tener estadísticas de las amenazas detectadas en los dispositivos.

La consola central de gestión debe permitir la configuración de los repositorios externos a la entidad de donde se descargarán las firmas de los clientes la cual será distribuidas ya sea por la consola o servidores de distribución internos.

La consola debe permitir registrar toda actividad realizada por cualquier usuario, con fecha y hora.

La consola debe permitir la creación de usuarios con privilegios limitados.

La consola debe permitirle al administrador delegar roles administrativos a los operadores de la Consola para administrar solo grupos específicos de nodos o agentes.

La consola debe tener Gestión de Cuarentena Local y Remota

La solución de consola debe permitirle al administrador ver las actividades de cada administrador y operadores de consola permitiendo la exportación de esta.

La consola debe ser capaz de crear grupos los cuales contengan uno o muchos nodos para fácil gestión basados en selección manual, información de software o cualquier propiedad personalizada.

Estos grupos personalizados se deben actualizar automáticamente una vez la información de software o cualquier propiedad personalizada sea cambiada.

La solución debe permitir ocultar el agente de la lista "Adicionar/Quitar Software" del panel de control.

La solución debe ser capaz de enviar logs y reportes en un formato entendible. En caso en que el formato no sea entendible, el proveedor o fabricante debe asistirnos/proveernos soporte para convertir los logs/reportes en el formato apropiado.

Las configuraciones realizadas en la consola de gestión no pueden poder ser cambiadas en los agentes por los usuarios (gestión centralizada).

La solución debe permitir la conexión en caso de falla del nodo de distribución principal a un segundo o tercer nodo más cercano, el cual debe poder ser definido por el administrador.

Si el cliente falla en comunicar su estado a la consola de gestión después de varios intentos, la consola debe marcar el agente de ese dispositivo como offline (fuera de línea) y después de un periodo extenso eliminarlo automáticamente de la consola. Los administradores se le deben permitir la definición de ese intervalo.

RENDIMIENTO

La solución de seguridad antivirus debe garantizar un bajo consumo de recursos de los equipos para que asegure su inicio rápido y un eficiente rendimiento sin interferir en el entorno de trabajo.

OTRAS ESPECIFICACIONES GENERALES.

La solución antivirus debe tener un motor de velocidad y precisión que mantenga los equipos seguros frente ataques, infiltraciones de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques provenientes de Internet sin entorpecer el rendimiento del sistema de los equipos.

Deberá detectar y eliminar/desinfectar al menos los siguientes tipos de amenazas: Spyware, Adware, Rogues, Ransomware, Keyloggers, Troyanos, Worms, Virus, etc.

La solución requerida debe tener integrado las siguientes funcionalidades para una óptima protección en el equipo, la red, internet y correo electrónico así:
Protección antivirus.
Protección Antispyware.
Filtrado de URL"s.
Protección del sistema de archivos en tiempo real.
Protección de documentos.
HIPS monitoreo de los sucesos dentro del sistema operativo.
Modo de presentación.
Protección Anti-Stealth.
Protección de acceso a la Web.
Protección del cliente de correo electrónico.

La solución antivirus debe permitir explorar y detectar infiltraciones dentro de archivos comprimidos con las siguientes extensiones de archivos: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO, BIN, NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE.

La solución antivirus debe contar con las funcionalidades capaces de estar alerta frente ataques y eventos sospechosos de software malicioso que ponga en peligro los equipos, capaces de eliminar proactivamente infiltraciones de virus, spyware, troyanos, gusanos, Adware, Rootkitsy otro ataques provenientes de internet sin entorpecer el rendimiento del sistema de los equipos.

La solución antivirus debe contar con un módulo de tareas programadas que permita configurar las diferentes frecuencias de actualización y horarios de análisis diarios, semanales, mensuales y manejo de horarios no laborales.

La solución antivirus debe permitir importar y exportar configuraciones.

La solución antivirus debe permitir, bloquear, o excluir direcciones URL.

La solución antivirus deberá permitir limitar el acceso mediante la selección de categorías de sitios web, basada en la clasificación automática en la nube, además de permitir crear reglas detalladas por grupos de usuarios y bloqueos de los sitios que generan un gran volumen de tráfico.
La solución antivirus deberá permitir definir redes de confianza.

La solución antivirus deberá contar con un firewall bidireccional que prevenga el acceso no autorizado a las redes de la

entidad.

La solución antivirus deberá tener proteger las comunicaciones de la entidad ante spam y amenazas provenientes del correo electrónico filtrando los protocolos POP3, IMAP, MAPI Y HTTP.

El módulo de protección del cliente de correo electrónico debe ser compatible con los siguientes clientes de correo electrónico Outlook de Office365.

Políticas y tareas granulares.

Antimalware con tecnología de punta (Análisis en tiempo real y análisis heurístico en busca de nuevas amenazas).

Cortafuegos Bidireccional (Analiza el trafico entrante y saliente, estableciendo reglas específicas para aplicaciones, puertos y direcciones ip).

Control web por palabras.

Control de aplicaciones (Permite bloquear cualquier aplicación que se ejecute en el equipo: Navegadores web, aplicaciones office, juegos etc.).

Control por palabras (Permite establecer control de palabras sobre el cliente de correo para evitar que se fugue información delicada para la compañía).

Inventario de software instalado en los equipos clientes.

Inventario de hardware (Memoria, disco duro, pantalla)

Instalación remota de software.

Bloqueo de puertos usb y autorun.

Los agentes no deben enviar ningún tipo de trafico broadcast.

El Endpoint debe contar con la certificación Gold OPSWAT para las categorías de antiphishing, antispyware, antivirus, cliente de copia de seguridad, cortafuego y filtrado de URLs.

ESPECIFICACIONES TÉCNICAS DE HARDWARE Y SOFTWARE

Procesadores soportados: lntel o AMO x86-x64.
Microsoft® Windows® Windows 7.0 - 8.0 - 8.1 Compatible para el nuevo Windows 10 - Soporte para base datos, My SQL, Oracle.

Software antivirus y antispyware debidamente licenciado, referenciado por Gartner y AVTEST, y que cuente con actualizaciones automáticas. Este programa deberá contar con respaldo y soporte directo del fabricante.

SERVICIO DE INSTALACIÓN

Servicio de implementación y configuración, en servidor local o en la nube, instalación en 670 máquinas de funcionarios.

CAPACITACIÓN

Capacitación presencial en la Entidad a dos funcionarios de TI donde explique la configuración y manejo del Antivirus políticas, reglas, objetos, administración general.

SOPORTE

5x8 del Antivirus Instalado, escalable según requerimientos del cliente. Para nuevas configuraciones o actualizaciones o el caso que sea crítico se debe realizar en sitio.

GARANTIA

La garantía y el soporte del antivirus deberán ser por un periodo mínimo de 12 Meses.

CONDICIONES MÍNIMAS GENERALES

El contratista deberá ejecutar el objeto del contrato cumpliendo cada una de las especificaciones técnicas y requerimientos mínimos de los ítems anteriores.

El contratista se compromete con la Entidad, a suministrar una solución de antivirus certificada y garantizada de fábrica, cumpliendo las Normas técnicas vigentes nacionales e internacionales y cumpliendo con todas las exigencias en materia de Antivirus.

El proponente debe comprometerse a entregar un informe de la instalación y configuración que se haya realizado en la Entidad.

El contratista deberá presentar claramente la metodología a seguir para: la Instalación, Ventanas de trabajo, cronograma, plan de trabajo, manual de procedimiento para administración de la herramienta y usuario final.