PLIEGO DE BASES Y CONDICIONES TECNICAS

CONSIDERANDOS INICIALES

1. El Poder Judicial de Tierra del Fuego será el usuario de los productos de software solicitados pudiendo el mismo instalarlos y utilizarlos en todos sus organismos dependientes.

2. Se contratará licenciamiento de uso por el Término de 1 (UN) año, con servicio de actualización de bases, definiciones y firmas de virus por el término de 1 (UN) año.

3. A efectos de centralizar la información, minimizar tiempos de aprendizaje y asignación de recursos humanos, se ponderarán únicamente aquellas ofertas que tengan todos los renglones de soluciones de software solicitados, en una única solución integrada. Se adjudicará a la oferta que resulte más conveniente.

4. PLAZO DE INSTALACIÓN: El plazo de instalación de la solución es de 90 (NOVENTA) días corridos computados a partir de la notificación de la Orden de Compra.

5. El proveedor brindará soporte técnico por el tiempo que dure el licenciamiento por mail y/o teléfono.

6. El proveedor deberá capacitar a un total de tres personas de los sectores de IT y Seguridad de la Información, durante el período contratado.

7. Idioma de las soluciones propuestas: ESPAÑOL e INGLÉS.

8. CONFIDENCIALIDAD: Toda la información a la que el prestador de cada servicio acceda con motivo de la prestación del servicio y/o quede bajo su guarda y conocimiento será considerada secreta y mantenida por la empresa en absoluta reserva y no la podrá suministrar a ninguna persona física y/o jurídica sin expresa autorización del Poder Judicial de Tierra del Fuego. El incumplimiento de lo descrito en el párrafo precedente provocará la rescisión del contrato y de corresponder, se dispondrán acciones legales por el daño ocasionado de acuerdo a la Ley de Protección de Datos Personales.

9. El proveedor debe contar con, al menos, dos (2) técnicos certificados por la marca en las soluciones ofertadas, en el país.

10. El ejecutor de los trabajos deberá poseer experiencia comprobable en instalaciones de estas características. Se requerirán asimismo antecedentes en la ejecución de por lo menos TRES (3) instalaciones de similar o mayor envergadura que la requerida. Se tendrán en cuenta las dimensiones de los proyectos presentados como antecedentes, y serán considerados sólo aquellos proyectos que se hallen terminados y entregados.

Alfonso Carolina
Auxiliar Área Contrataciones
Superior Tribunal de Justicia

1.1.2. La consola de monitoreo y configuración deberá ser a través de una central única, basada en web y en nube o modalidad on premise, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos;

1.1.3. La consola deberá presentar un tablero de control con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional;

1.1.4. La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos;

1.1.5. Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.

1.1.6. Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales;

1.1.7. La instalación debe poder realizarse de forma manual obtenida a través del cliente descargado de la consola central o también vía correo electrónico. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.

1.1.8. Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos;

1.1.9. Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.

1.1.10. La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros;

1.1.11. Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador;

1.1.12. Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.

1.1.13. Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.

1.1.14. Permitir la exportación de los informes gerenciales a los formatos CSV y PDF;

Alfonso Carolina
Auxiliar Área Contrataciones
Superior Tribunal de Justicia

1.1.25. Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses;

1.1.26. Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF;

1.1.27. Debe contener varios informes para el análisis y control de los usuarios y endpoint. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints;

1.1.28. Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF

1.1.29. Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.

1.1.30. Deberá tener la posibilidad de instalar un servidor para reenvío de eventos en caso de que el agente no pueda comunicarse con la consola en la nube.

2. Características básicas del agente de protección contra malware:

2.1.1. Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido;

2.1.2. Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque;

2.1.3. Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA);

2.1.4. Debe proteger las funciones críticas en los navegadores de Internet;

2.1.5. Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos;

2.1.6. Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA);

2.1.7. Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección;

2.1.8. Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en

Alfonso Catalina
Auxiliar Area Contrataciones
Superintendencia de Salud

4.1.3. Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.

5. Debe contar con capacidades de EDR y XDR

La tecnología EDR detecta ataques que un antivirus ha pasado por alto. Monitoriza y evalúa todas las actividades de la red (eventos de los usuarios, archivos, procesos, registros, memoria y red). Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

Se entiende como XDR (detección y respuesta extendidas) recopila y correlaciona automáticamente datos en múltiples capas de seguridad: email, endpoint, servidor, workload en la nube y la red. Esto permite una detección más rápida de las amenazas y una mejor investigación y tiempos de respuesta mediante un análisis de seguridad.

6. El analista de seguridad debe poder identificar qué atributos de código de un objeto son similares a archivos "known-good" y "known bad" con esto se puede determinar si se pueden permitir o bloquear.

6.1.1. Debe tener un Sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints con información detallada del malware en sí y el origen de la infección (explorador de Windows, correo electrónico, navegador, etc.)

6.1.2. Debe permitir una investigación guiada entregando visibilidad de la dimensión del ataque cómo inicia, cómo impacta, cómo se responde.

6.1.3. Detectar ataques que pueden haber pasado desapercibidos.

6.1.4. Buscar de forma proactiva (Threat Hunting) indicadores de compromiso por nombre de archivo, SHA, direcciones IP.

6.1.5. Priorizar eventos para investigación.

6.1.6. Poder aislar una máquina comprometida de la red de forma automática mientras la investigación del incidente se realiza.

6.1.7. Poder generar un Snapshot (copia instantánea) forense durante una investigación de una amenaza.

6.1.8. Poder realizar consultas de cumplimiento de estándares de seguridad.

6.1.9. Poder realizar consultas de técnicas y tácticas de ataque mapeadas en MITRE ATT&CK.

6.1.10. Poder realizar consultas de conexiones de Red y transferencias de archivos.

6.1.11. Poder realizar consultas sobre información del SO, servicios, parches y más.

Altonso Carolina
Auxiliar Área Contrataciones
Superior Tribunal de Justicia

seguridad perimetral.

- Se deberá contar con doble factor de autenticación para acceso a la consola
- La solución deberá soportar Android, iOS.
- La consola cloud podrá accederse desde cualquier dispositivo
- Debe contar con integración con Active Directory y LDAP
- Deberá contar con un módulo de reporteo integrado en la misma consola
- Los reportes podrán generarse por dispositivo o grupo de ellos
- La consola de administración deberá contar con distintos roles de acceso
- El enrolamiento de los dispositivos deberá realizarse por código URL
- La consola deberá estar en español

PERFILES

- La solución debe permitir bloquear ejecución de JavaScript en el navegador
- La solución deberá bloquear la instalación de aplicaciones de fuentes desconocidas

SEGURIDAD

- En Android y iOS deberá contar con antivirus
- El antivirus deberá contar con protección en tiempo real
- La protección antimalware deberá contar con Machine Learning/Deep Learning
- El módulo de antivirus debe tener la capacidad de escanear las aplicaciones ya instaladas
- Deberá proteger de aplicaciones maliciosas y de baja reputación
- Deberá prevenir el acceso a sitios maliciosos o de baja reputación
- Deberá contar con Antiphishing
- Deberá contar con protección web
- La solución deberá reportar a través de un scoring aquellas aplicaciones potencialmente maliciosas.

CIFRADO / ENCRIPTACIÓN DE DATOS

1 **ASPECTOS GENERALES**

1.1 Debe tener la capacidad de cifrar el disco completo, reemplazando el Máster Boot Record (MBR)

1.2 La solución debe proveer mecanismos seguros que garanticen la recuperación del acceso en caso de pérdida de la contraseña. Estos mecanismos deben requerir la intervención y el intercambio de información con la consola de administración.

1.3 Debe ser capaz de descifrar el disco en forma automática, desde la consola de administración y mediante mecanismos manuales

1.4 La solución debe solicitar autenticación al usuario antes de iniciar la carga del sistema operativo (SO). Luego de iniciar el SO, la solución debe poder configurarse de manera que solicite o no, nuevamente, las credenciales de autenticación del usuario.

Alfonso Carolina
Auxiliar Area Contrataciones
Superior Tribunal de Justicia

una imagen protegida del disco encriptado, como:

- Guidance Software (EnCase)

5.3 La solución debe soportar el Trusted Platform Module (TPM) de Intel

5.4 La solución debe integrarse con Microsoft Applocker

5.5 La solución debe integrarse con la herramienta de administración de VPRO del mismo fabricante

5.6 La solución debe permitir el manejo de cifrado nativo BitLocker y FileVault, brindado por Microsoft y Apple, respectivamente

6 GESTION

6.1 El producto debe ser administrado desde la misma consola centralizada utilizada para las demás soluciones de protección del endpoint (Antivirus, Antispyware, HIPS, DLP y Control de Aplicaciones, entre otras)

6.2 La solución debe contar con una herramienta externa que utilice las Llaves de Encripción almacenadas en la consola de administración para ejecutar cualquier actividad de recuperación de discos o archivos.

6.3 La solución debe soportar Single Sign-On (SSO) en integración con las políticas de grupo (GPO) del Directorio Activo de Microsoft.

6.4 La solución debe soportar los siguiente tokens o herramientas de Autenticación SSO:

- ActivIdentity/DOD CAC (PKI)
- CAC Schlumberger Access 32k v2
- Axalto Access 64k
- Oberthur ID One v5.2
- Gemalto 64k v2
- Starcos 2.1 T=1 2.1 T=1
- PIV PKI 2048 Oberthur CS PIV
- Safesign PKI Smart Card Evoniks
- Aladdin eToken Pro 64K (Card OS 4.01, 4.2, 4.2b) (Q0058)
- Aladdin eToken Pro 32K (Card OS 4.01, 4.2, 4.2b) (Q0088\68)
- RSA SID800
- eGate certificate smart card

6.5 La solución solo debe poder removerse del sistema por un usuario administrador y remotamente.

6.6 La solución debe contar con la opción de generar un "código de respuesta" para la recuperación del administrador

6.7 El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles

6.8 La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global

7 REPORTES

7.1 La solución debe proveer reportes del estado de la solución en las máquinas administradas. Todos estos reportes deben ser exportables vía correo ó a documentos XML, PDF y XLS.

Alfonso Carolina
Auxiliar Área Contrataciones
Superior Tribunal de Justicia

1. Se deberá asistir en la instalación de las soluciones adquiridas por un tiempo mínimo de 120 horas en las cuales se realizarán la instalación e implementación como la configuración inicial de los productos.
2. Dicha asistencia podrá ser remota o presencial con parámetros de acceso a definir por parte de este organismo.

CERTIFICACIÓN OFICIAL DE LA SOLUCIÓN INSTALADA

1. Se deberá proveer el certificado oficial de la marca una vez instalados todos los agentes adquiridos, para lo cual se efectuará una auditoría a fin de garantizar la correcta instalación y configuración de los mismos.

SERVICIO REMOTO DE CONTROL, GESTIÓN Y ADMINISTRACIÓN POR 12 MESES

1. Se deberá proveer un servicio por 12 meses de asistencia para el control, gestión y administración de las soluciones adquiridas e instaladas.
2. El esquema de soporte será de 8x5 (8 horas diarias x 5 días hábiles)
3. La prestación del servicio será de forma remota y/o presencial de ser necesario.
4. Los incidentes podrán ser reportados vía: teléfono, email, mensajería instantánea o por una web propia del proveedor donde se reportan los incidentes.
5. El tiempo de respuesta requerido es de 6 horas máximo en horas y días de servicio en caso de incidentes considerados severos.
6. Los medios por los que se proveerá la solución serán por conexión remota, email o cualquier otro medio de comunicación.
7. El servicio deberá ser prestado por un especialista certificado en los productos contratados.
8. Los servicios que deberán ser prestados además son:
    a. Asistencia para la actualización de nuevas versiones.
    b. Informe de vulnerabilidades y actualizaciones
    c. Asistencia en cambios de políticas de configuración
    d. Resolución de problemas de configuración.
    e. Diagnósticos en general.----------

Alonso Carolina
Auxiliar Área Contrataciones
Superior Tribunal de Justicia