ADQUISICIÓN DE HERRAMIENTAS AVANZADAS PARA EL DESBLOQUEO Y ACCESO FORENSE A DISPOSITIVOS MÓVILES INCLUYENDO AQUELLOS DE SISTEMA OPERATIVO IOS

Los oferentes interesados deben presentar su propuesta económica en este espacio.
NOTA: Una vez diligenciada la propuesta económica, este debe ser presentada en formato .pdf, sin realizar ningún tipo de modificación en su estructura. Cualquier alteración puede ser causal de rechazo de la propuesta.

ÍTEM	REQUERIMIENTO MÍNIMO	CUMPLE	NO CUMPLE
ESPECIFICACIONES			
1.	Cantidad: dos (2).		
2.	Marca: especificar.		
3.	Modelo y/o referencia: especificar.		
4.	Tiempo de soporte y garantía: 36 meses.		
5.	**Nombre Comercial del Bien o Servicio** Herramienta forense para desbloqueo, extracción avanzada y análisis de evidencia digital de dispositivos móviles.		
6.	**Calidad** El sistema forense ofertado debe haber sido evaluada en los últimos tres (3) años (por el Departamento de Seguridad Nacional de los Estados Unidos en la categoría JTag y ChipOff (https://www.dhs.gov/publication/st-binary-image-jtag-chip-decoding- and-analysis-tool) en la categoría "Mobile Device Acquisition Tool" (https://www.dhs.gov/publication/st-mobile-device-acquisition). Será descalificada la propuesta que no tenga sus pruebas en ambas categorías posteriores a 2022 en la página online del DHS.		
7.	**Generalidades** Adquisición de herramienta forense para desbloqueo, extracción avanzada y análisis de datos de dispositivos móviles (teléfonos celulares, tabletas digitales, teléfonos satelitales, avantel, drones y sus elementos anexos como tarjeta SIM o tarjeta de memoria extraíble) que garantice la integridad del contenido del dispositivo objeto de estudio (no dejar rastro ni alterar contenido).		
8.	**La herramienta forense requerida debe estar compuesta por:** Software de extracción		
	Software de decodificación y análisis		
	Accesorios (cables, conectores, adaptadores, cargadores, entre otros) que sean necesarios para la conexión de los dispositivos móviles a la estación de cómputo.		
9.	**Optimización:** Con el objetivo de que la entidad **no** adquiera equipos de cómputo adicionales el software de extracción se **debe poder** instalar en las estaciones de cómputo actuales de la entidad.		
10.	**Aclaración:** Cuando se hace referencia a dispositivos móviles se incluyen: teléfonos celulares, teléfonos satelitales, avantel, tabletas digitales, GPS, Drones, entre otros, con sus respectivos elementos accesorios (tarjeta SIM y memoria de almacenamiento extraíble). La herramienta forense para extracción y análisis de datos de dispositivos móviles como mínimo debe:		

	Extraer datos de dispositivos móviles con diferentes sistemas operativos.		
	Extraer datos de dispositivos móviles con diferentes marca y modelos.		
	Extraer datos de dispositivos móviles con bloqueos de seguridad activados, tales como: patrón, contraseña, reconocimiento facial, pin, entre otros.		
	Contar con mecanismos incorporados en la misma herramienta forense que permitan documentar información de forma manual (fotografía, video, captura de pantalla)		
	Realizar cálculo de valor HASH a los archivos de datos (imágenes, videos, audios, documentos, entre otros) extraídos de los dispositivos objeto de estudio.		
	Nota: Es importante aclarar que “Extraer” hace referencia al proceso de obtener la información almacenada en el dispositivo móvil a través de los procesos automáticos que corre la herramienta forense, por tanto, no se considera extracción a la información obtenida mediante otros mecanismos que pueden estar implementados en la misma herramienta como son toma de imágenes, video o captura de pantalla.		
	Desactivar, obtener o saltar bloqueos de seguridad (patrón, contraseña, reconocimiento facial, pin, entre otros.) y extraer la información contenida en el dispositivo móvil objeto de estudio,		
	Identificar por un proceso de fuerza bruta, es decir intentando múltiples claves posibles de acuerdo al tipo de contraseña con la que se encuentre protegido el dispositivo objetivo, sin que se lleve un registro de cuales o cuantos códigos diferentes se intentan, esto, con el fin de encontrar cual de todas las posibilidades que se intenten durante el proceso de fuerza bruta corresponde al código de bloqueo correcto y se pueda realizar extracciones completas del sistema de archivos en dispositivos con cifrado FDE y FBE.		
	Permitir el análisis de datos de múltiples orígenes como son: dispositivos móviles y backups, entre otros		
	Decodificar la información extraída		
	Recuperar información borrada de los dispositivos móviles		
	Reconstruir información eliminada de los dispositivos móviles (data carving, metacarving, location carving). La solución deberá ser capaz de decodificar datos de aplicaciones no soportados, a través del reconocimiento automático de patrones en el Código de las aplicaciones.		
	Decodificación (apertura), lectura y análisis del contenido de los archivos de extracción obtenidos con la herramienta base que ha manejado la Entidad durante los últimos cinco (5) años.		
	Combinar en un solo archivo varias extracciones realizadas a un mismo dispositivo móvil y sus componentes como Tarjeta SIM y Memoria extraíble con el fin de generar un único reporte, Generar reportes de manera organizada y en diferentes formatos como PDF, HTML, XLS, UFDR, entre otros. Generar archivos de caso portable en el que se puedan aplicar filtros, búsquedas, selecciones y generar reportes en formatos PDF, HTML, XLS, UFDRs entre otros. Contar con todos los accesorios necesarios para el correcto funcionamiento de la herramienta forense. Contar con el lector/bloqueador de tarjeta SIM en sus diferentes referencias (nano SIM, micro SIM, SIM). Contar con todos los cables que permitan la conexión de los diferentes dispositivos móviles para la extracción de la información. Contar con batería portable con sus respectivos cables o conectores de alimentación para los dispositivos móviles existentes en el mercado, Soportar la extracción de información, decodificación y análisis de mínimo 34.000 referencias de dispositivos móviles.		

	Se debe contar con al menos dos niveles de soporte para la Herramienta, uno por correo o teléfono y un segundo nivel presencial.		
11.	**Requisitos específicos** La herramienta forense para extracción y análisis de datos de dispositivos móviles debe cumplir con los siguientes requisitos específicos mínimos: Métodos de extracción		
	Lógica		
	Sistema de archivos		
	Física		
	Extracción Parcial BFU en dispositivos iOS Bloqueados		
	Captura de chats: Capturas de pantallas de chats en forma automatizada.		
12.	**Adquisición de Datos:** Dispositivos con sistemas operativos: iOS, Android, Windows Phone, Windows Mobile, BlackBerry, Symbian, sus variaciones y otros sistemas operativos que surjan en el mercado durante el tiempo de vigencia de la licencia.		
	Dispositivos Bloqueados con Procesador Qualcomm Cifrados.		
	Dispositivos Bloqueados con Procesador Exynos Cifrados.		
	Dispositivos Bloqueados con procesador MTK Cifrados.		
	Dispositivos Bloqueados con procesador Hisilicom Cifrados.		
	Dispositivos genéricos o chinos.		
	Desactivar, obtener o saltar bloqueos de seguridad (patrón, contraseña, reconocimiento facial, pin, entre otros.) y extraer la información contenida en el dispositivo móvil objeto de estudio		
	Ataques de fuerza bruta en referencias seleccionadas de dispositivos FBE para encontrar la contraseña y extraer la información contenida.		
	Decodificación,(apertura), lectura y análisis de las extracciones realizadas con la herramienta base que ha manejado la Entidad durante los últimos cinco (5) años.		
13.	**Datos Extraídos:**		
	Sistema de archivos		
	Contactos		
	Mensajes de texto		
	Calendarios, notas y tareas		
	Diccionario de usuario		
	Soporte para Apps		
	Detección de malware en los sistemas operativos iOS, Android e blackberry.		
	Passwords		
	Datos borrados		
	Datos reconstruidos		
	Datos de SQLite		
	Datos de Plist		
	Redes sociales		
	Aplicaciones de mensajería instantánea incluyendo archivos de datos adjuntos (imagen, video, audio, documentos) y generación de reportes organizados y comprensibles.		

	Historial de Internet		
	Registro de ubicaciones geográficas por medio de torres de comunicación, GPS o redes WIFI (BSSID).		
14.	**Extracción de datos de autenticación de servicios en la nube (Cloud) almacenados en los dispositivos móviles objeto de estudio para:**		
	Extracción de datos desde servicios de almacenamiento de Apple, Microsoft, Google, entre otros obtenidos a través de la utilización de un paquete de credenciales generado por la solución.		
	Redes sociales		
	Backup de iCloud y Windows Phone		
	Archivos entregados como resultado de una carta rogatoria o una orden judicial a proveedores de servicios en la nube como Facebook y Google		
	En caso de no Deberá ser presentada una carta de compatibilidad emitida por los fabricantes de la solución propuesta y de la solución existente confirmando la compatibilidad entre las soluciones.		
15.	HASH calculado por la misma herramienta a los archivos de datos extraídos del dispositivo móvil objeto de estudio.		
	Aplicando mínimo dos (2) algoritmos (MD5, SHA-1, SHA-256).		
16.	Análisis de Backups no cifrados		
	Imágenes y backups de iOS y Android		
	Backups de: BlackBerry (BBB – IPD)		
	Imágenes JTAG y Chip-Off		
	Archivos binarios (.bin)		
	Archivos comprimidos (.zip, tar, rar)		
	Análisis de Backups cifrados		
	Recuperación de contraseñas Android (ADB)		
	Recuperación de contraseñas de imágenes de Android.		
17.	**Geo-Localización**		
	Visualización de rutas		
	Visualización de metadatos de geo-localización en los archivos de datos.		
	Mapas sin conexión		
	Servicio online de conversión de identificadores de torres de telefonía celular en coordenadas geográficas		
	NOTA: La herramienta ofertada deber ser la última versión liberada por el fabricante, se verificará en la página web del fabricante.		
18.	**Análisis de Datos:**		
	Búsqueda de datos (búsquedas por palabras clave, HASH, números, patrones, entre otros).		
	Filtros de imágenes por tamaño y por ruta		
	Análisis de registros de llamada		
	Líneas de tiempo		
	Conexión proyecto VIC		
	Búsqueda automatizada de criptomonedas		
	Virtualizador de Android para aplicaciones		
	Decodificar la información extraída, permitiendo la traducción automática entre idiomas distintos tales como español e inglés.		
19.	**Transferencia de conocimiento:**		

	El contratista se compromete a realizar una transferencia de conocimiento sobre el uso y manejo de la herramienta adquirida, dirigida a un mínimo de cinco (5) funcionarios designados por la entidad contratante. Esta capacitación deberá cumplir con los siguientes criterios: **Intensidad Horaria:** La capacitación tendrá una duración mínima de ocho (8) horas, distribuidas de manera que permita una comprensión completa y práctica de las funcionalidades y aplicaciones de la herramienta. **Calificación del Instructor:** El personal que llevará a cabo la capacitación debe estar certificado por el fabricante de la herramienta, garantizando así un nivel de expertise adecuado y la actualización constante sobre las últimas funcionalidades y mejores prácticas del uso del sistema. **Certificación en Fundamentos Forenses:** Además, el instructor debe contar con un certificado en fundamentos forenses, asegurando que posea los conocimientos necesarios para instruir en las técnicas y principios de la extracción y análisis de datos forenses. **Documentación de Certificación:** Se deberá proporcionar evidencia documental de la certificación del instructor tanto en el uso de la herramienta como en fundamentos forenses.		
20.	**Garantía** La garantía del sistema deberá tener la misma vigencia que los años de licenciamiento adquiridos.		
21.	**Empaque y rotulado** Maletín para porte y transporte		
22.	**Presentación y Unidad de Medida** Un dongle y kit de accesorios por cada licencia de suscripción de software con vigencia de soporte y actualizaciones por el tiempo estipulado en el contrato – Unidad.		
23.	**Sistema de integración con unidades de extracción forense ya existentes en la institución** La solución debe permitir realizar extracciones físicas, completas del sistema de archivos (Full File System), extracciones completas después del primer desbloqueo (AFU), con acceso avanzado en dispositivos Android y iOS bloqueados en el estado antes del primer desbloqueo (BFU). El contratista debe entregar todas las licencias de software y el hardware necesario (adaptadores, cables, etc.), para el óptimo funcionamiento de la solución.		
24.	**Especificaciones de acceso avanzado** La solución debe reconocer los diferentes sistemas de protección de acceso en los dispositivos móviles (PIN, PATRON, CONTRASEÑA). **Android:**		

- La solución debe ser capaz de realizar extracciones físicas en dispositivos con cifrado FDE o extracciones completas del sistema de archivos (Full File System) en dispositivos con cifrado FDE o FBE, como por ejemplo en dispositivos Samsung, Huawei, Xiaomi, Motorola, LG, OPPO, Nokia, ZTE, OnePlus, VIVO, Alcatel y otros fabricantes que tengan hasta la versión 14 de Android.

- La solución debe ser capaz de realizar extracciones completas después del primer desbloqueo en dispositivos Android bloqueados pero que no han sido apagados de manera manual o por falta de batería manteniendo las propiedades y las llaves de cifrado en memoria volátil (AFU), como por ejemplo en dispositivos Samsung, Huawei, Xiaomi, Motorola, LG, OPPO, Nokia, ZTE, OnePlus, Vivo, Alcatel, Realme, Tecno, y otros fabricantes.

- La solución debe ser capaz de atacar por fuerza bruta el mecanismo de seguridad adicional conocido como el inicio seguro de Samsung (Samsung Secure Startup) en dispositivos Samsung con Procesadores (Chipsets) Qualcomm y Exynos.

- La solución debe ser capaz de atacar por fuerza bruta la seguridad de dispositivos Samsung con cifrado FDE y FBE que vengan fabricados con procesadores (Chipsets) Qualcomm y Exynos para obtener la información almacenada en estos dispositivos.

- La solución debe ser capaz de atacar por fuerza bruta la seguridad de dispositivos Huawei con procesador (Chipset) Kirin y Qualcomm para obtener la información en el dispositivo.

- La solución debe ser capaz de atacar por fuerza bruta la seguridad de dispositivos Motorola, LG, Nokia, y de otros fabricantes con procesador (Chipset) Qualcomm cifrados con FBE para obtener la información en el dispositivo.

- La solución debe ser capaz de atacar por fuerza bruta u omitir la seguridad de dispositivos Motorola, LG, Nokia, y de otros fabricantes con procesador (Chipset) Qualcomm cifrados con FDE para obtener la información en el dispositivo.

- La solución debe ser capaz de atacar por fuerza bruta el mecanismo de seguridad adicional conocido como el inicio seguro (Secure Startup) en dispositivos Android con cifrado FDE y que vengan con Procesadores (Chipsets) MTK de fabricantes como por ejemplo Motorola, LG, Nokia, Huawei y otros.

- La solución debe poder identificar, extraer y descifrar el contenido de la carpeta segura de dispositivos Samsung (Samsung Secure Folder).

- La solución debe poder identificar, extraer y descifrar el contenido de la carpeta segura de dispositivos Huawei (Huawei Private Space).

- La solución debe poder identificar, extraer y descifrar el contenido de la carpeta segura de dispositivos Xiaomi (Xiaomi Second Space).

iOS:

	• Atacar por fuerza bruta la seguridad de dispositivos iOS en estado (BFU), desde el iPhone 5 hasta el iPhone 11 con versión de iOS 18.2.1 para determinar el código de bloqueo del dispositivo, descifra, extrae y decodifica la informacion. • Realizar extracciones completas después del primer desbloqueo en dispositivos (AFU) desde el iPhone 6 hasta el iPhone 15 iOS 18.2.1, que no han sido apagados de manera manual o por falta de batería manteniendo las propiedades y las llaves de cifrado en memoria volátil. • Realizar una extracción completa del Sistema de archivos (Full File System) de dispositivos iOS desde el iPhone 5 hasta el iPhone 15 iOS 18.2.1 una vez se encuentre el código de desbloqueo o que se encuentre previamente desbloqueado. • Capacidad de ejecutar ataques de fuerza bruta tanto de forma autónoma (El proceso de fuerza bruta ocurre en el teléfono objetivo) como también de forma conectada al adaptador de la solución. • La solución debe generar un archivo de extracción, que garantice poder ser procesado en un software de decodificación y análisis de forma totalmente local.		
25.	**Otras especificaciones** • El fabricante deberá publicar periódicamente durante el periodo de la licencia, nuevas versiones con el objetivo de ampliar el alcance de acceso a modelos y versiones de sistemas operativos de dispositivos iOS y Android más recientes. • La solución debe venir protegida desde la fábrica. • Se debe proveer un adaptador para los dispositivos móviles previamente preparado y robustecido por fábrica. • El adaptador de la solución incluirá cables propios de fábrica. • La solución debe funcionar con una conexión a internet abierta de al menos 40 Mb de ancho de banda. • El proveedor deberá realizar una transferencia de conocimiento a mínimo 10 funcionarios, con una intensidad horaria mínimo de 8 horas. • La solución debe incluir las actualizaciones de hardware (cables y adaptadores) por los **36** meses de la suscripción. • La solución debe realizar las extracciones de manera forense para que la información obtenida tenga la mayor validez posible en procesos legales, administrativos u otros en los que se pueda aprovechar la información. • El oferente deberá presentar documento del fabricante certificando que cumple con todos los ítems de las especificaciones técnicas.		

	• El proponente deberá certificar la educación con título recibida en entidades debidamente reconocidas ante el ministerio de educación del funcionario el cual realizara la instalación y capacitación de la solución, asociada nivel de pregrado En ingeniería de sistemas y/o telecomunicaciones y/o Electrónica y/o Mecatrónica y/o áreas afines, para lo anterior el proponente deberá anexar copia de los diplomas (mínimo 1) que acrediten su idoneidad en cualquiera de las ramas indicadas. • Con el fin de garantizar la idoneidad del personal profesional que se vincula al proyecto el proponente deberá anexar mínimo un (1) certificado emitido por fabrica como operador.		
26.	**Certificación de Licenciamiento** Se debe certificar mediante documento, el cual acredite la autenticidad de la licencia, derechos de autor del fabricante y certificado de distribuidor autorizado en Colombia. De igual forma la licencia no debe tener limitaciones a la cantidad de procesos de desbloqueo que se ejecuten con la herramienta de desbloqueo. Lo anterior con el fin que el proveedor, garantice a la entidad; la legitimidad de las licencias, salvaguardándola de cualquier responsabilidad por el uso del software.		
27.	El oferente deberá adjuntar junto con la oferta la ficha técnica original por parte de fábrica.		
28.	**Experiencia** El oferente deberá contar con un ingeniero de planta de más de 5 años de experiencia laboral en carreras afines a ingeniería eléctrica, electrónica, mecatrónica, con especialización en gerencia de proyectos. El oferente deberá contar con un especialista de producto de planta, certificado por el fabricante en el uso de la herramienta y además en fundamentos forenses. Este especialista brindará soporte a los usuarios finales, garantizando que cuenten con una experiencia respaldada por su certificación.		
29.	**Proponente** Se deberá acreditar experiencia en un contrato, cuyo valor sea igual o mayor al 100% del valor del presupuesto oficial, expresados en SMMLV del año de ejecución del contrato, cuyos objetos estén relacionados con adquisición de software de desbloqueo avanzado y extracción de datos de dispositivos móviles de alta gama Android y IOS		

ÍTEM	CONDICIONES TÉCNICAS ADICIONALES	CUMPLE	NO CUMPLE
30.	El oferente se compromete a entregar bienes de óptimos estándares de calidad, reconocidos en el mercado y con el respectivo registro.		
31.	El contratista estará obligado a garantizar a la Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL la legitimidad de las licencias, salvaguardándola de cualquier responsabilidad por el uso del programa motivo de la adquisición.		

32.	El contratista garantizará que los elementos tecnológicos (cables, dongle y demás dispositivos que garantizan el adecuado funcionamiento de la herramienta) deberán ser de marcas reconocidas y con soporte y garantía técnica en el mercado colombiano, deberán ser originales, nuevos, no re manufacturados en Colombia y en otros países, de la misma marca de los equipos objeto de este contrato, necesarios para su correcto funcionamiento, estos deberán tener garantía y serán sin costo adicional para la Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL. Luego del cambio de una parte (repuesto), debe quedar operando y en funcionamiento. De igual forma, junto con su oferta deberá adjuntar la ficha técnica o enlace web para cada equipo ofertado donde se puedan evidenciar a su vez marca, modelo y referencia.		
33.	El contratista debe colocar a disposición de la Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL los siguientes medios de manera permanente (7X24): línea telefónica (celular y fijo) y correo electrónico, que garanticen la comunicación permanente con el CIBER GAULA - Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL y/o supervisor del contrato, con el fin de poder reportar los incidentes que se presenten y estar en comunicación permanente para cualquier eventualidad o soporte que se presente. La firma contratista deberá garantizar que el bien se oriente a que, si se presenta una falla inherente a la fabricación y que redunde en la seguridad del equipo, esta sea cambiada sin costo alguno. Para el mantenimiento por defecto de fábrica o falla del mismo el servicio deberá ser las 24 horas con respuesta inmediata a las llamadas de emergencia durante el tiempo de ejecución del contrato. La firma contratista deberá dar respuesta en un mínimo tiempo para atender los requerimientos por fallas que se presenten, durante el tiempo de la garantía del software.		
34.	El oferente debe **certificar** que se compromete a sostener los precios de la oferta durante la ejecución del contrato.		
35.	**CALIDAD Y CAMBIO Y/O REPOSICIÓN DE LOS ELEMENTOS** El oferente debe **anexar certificación** de que aun cuando los elementos objeto del proceso cumpliendo con todas las especificaciones técnicas al momento de su entrega a la Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL, llegasen a presentar defectos de fabricación en sus características, el oferente efectuara su cambio, sin costo alguno para la Dirección de Antisecuestro y Antiextorsión – POLICIA NACIONAL en un término no mayor a quince (15) días hábiles, previa coordinación y solicitud con el supervisor.		
36.	El fabricante deberá emitir una certificación donde conste que para cada herramienta de manera independiente no se cuenta con limitaciones técnicas ni comerciales respecto a la cantidad de procesos de desbloqueo realizados. Esto incluye: Uso ilimitado: Ejecución de procesos de desbloqueo sin restricción numérica de dispositivos o intentos. Ausencia de costos por uso: La herramienta no deberá requerir el pago de consumibles digitales (créditos, tokens o similares) para la ejecución de sus funciones de desbloqueo. Disponibilidad Funcional: No se permitirán bloqueos de funcionalidad basados en cuotas diarias, mensuales o anuales de procesamiento.		