AVISO DE CONTRATACIÓN PÚBLICA PREVISTA- SUBASTA INVERSA ELECTRÓNICA
No. SIE-INEC-027-2022

El INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS, en cumplimiento a lo establecido en el Apéndice 4, Anexo XII del "ACUERDO COMERCIAL ENTRE LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS, POR UNA PARTE, Y COLOMBIA, EL PERÚ Y ECUADOR, POR OTRA", procedió con la revisión del CPC y el umbral del Presupuesto Referencial y define a la contratación de LICENCIAS PARA EL ANÁLISIS Y CONTROL DE VULNERABILIDADES DE LA INFRAESTRUCTURA, BASE DE DATOS Y APLICATIVOS DEL PROYECTO CPV, se encuentra cubierta por el Acuerdo Comercial; por lo que, expide el siguiente aviso de contratación pública prevista:

OBJETO DE CONTRATACIÓN: LICENCIAS PARA EL ANÁLISIS Y CONTROL DE VULNERABILIDADES DE LA INFRAESTRUCTURA, BASE DE DATOS Y APLICATIVOS DEL PROYECTO CPV

DATOS DE LA ENTIDAD CONTRATANTE:	
Nombre de la Entidad Contratante:	INSTITUTO NACIONAL DE ESTADISTICA Y CENSOS
Ruc:	1768038270001
Dirección:	País: Ecuador. Provincia: Pichincha. Ciudad: Quito Dirección: Juan Larrea N15-36 y Jose Riofrio
Teléfono:	(02) 2544-326
Contacto:	marcela_carrera@inec.gob.ec
Costo por edición de documentación del proceso de contratación	$0,00

Objeto de Contratación:	LICENCIAS PARA EL ANÁLISIS Y CONTROL DE VULNERABILIDADES DE LA INFRAESTRUCTURA, BASE DE DATOS Y APLICATIVOS DEL PROYECTO CPV
Código de Proceso en SERCOP	SIE-INEC-027-2022
Código CPC Nivel 5	51290
Tipo de procedimiento	Subasta Inversa Electrónica
Monto sin IVA	$ 260.000.00 (Doscientos sesenta mil dólares de los Estados Unidos de América, con 00/100)
Condiciones de Pago	El Instituto Nacional de Estadística y Censos se compromete a pagar el 100% del contrato, a la entrega recepción de las licencias, debidamente instaladas y configuradas para el análisis y control de vulnerabilidades de la infraestructura, base de datos y aplicativos del proyecto CPV, previa suscripción del Acta de Entrega Recepción Definitiva y presentación de la factura correspondiente.
Plazo de Ejecución	37 días de calendario, desde el día siguiente de la fecha de suscripción del contrato.
Cantidad de mercadería o servicio objeto de la contratación	**Servicio Esperado:**

ITEMS	DESCRIPCIÓN	CANTIDAD REQUERIDA
SISTEMA DE PROTECCIÓN DE BASE DE DATOS	LICENCIA	1
HERRAMIENTA DE ANÁLISIS ESTÁTICO Y DINÁMICO	LICENCIA	1

CORRELACIONADOR DE EVENTOS	LICENCIA	1

SISTEMA DE PROTECCIÓN DE BASE DE DATOS
El sistema debe incluir la característica de despersonalización de datos y enmascaramiento de datos personales en ambientes no productivos
El sistema debe permitir el descubrimiento de datos sensibles para mínimo 5 instancias de bases de datos.
El sistema debe permitir la protección de datos personales en ambientes productivos y desarrollo para mínimo 5 instancias de bases de datos.
El proveedor deberá configurar mínimo 3 instancias de bases de datos definidas por el INEC.
El licenciamiento de la protección de Base de Datos debe ser perpetuo con licenciamiento de soporte de mínimo 2 años.
El sistema debe ser Compatible con Hadoop, Oracle, DB2, MySQL, IDMS, Sybase, Microsoft SQL, Azure SQL y cualquier base de datos tradicional.
El sistema debe ser instalado en la infraestructura del INEC en modo virtual.
El sistema debe permitir configurar políticas de cifrado, tokenización y administración de claves que se controlan de forma centralizada, lo que permite que la política de privacidad de datos se defina, aplique, audite y administre de forma centralizada para la protección de datos estructurados.
El sistema debe permitir el cifrado de plataformas nativas para mayor eficiencia en una amplia gama de servidores de aplicaciones.
El sistema debe permitir la protección de datos estructurados y no estructurados consistentes y compatibles en Windows, Linux, AIX, Solaris, HP/UX, HPE NonStop, Stratus VOS, IBM z/OS, AWS, Azure, Hadoop y Teradata.
Anonimización, cifrado y tokenización de información de datos estructurados
El sistema debe contar con soporte nativo y herramientas de integración de API para todas las plataformas empresariales y sistemas operativos contemporáneos con cifrado y seudonimización que se pueden integrar fácilmente en los procesos de manejo de datos, sistemas de producción y aplicaciones.
El sistema debe permitir la preservación del formato basado en el estándar NIST SP 800-38G comúnmente conocido como el modo FFX de AES.
El sistema debe contar con la tecnología Secure Stateless Tokenization (SST)

	El sistema debe contar con protección de tokenización donde cifra con AES 256 cuando se almacena.
	El sistema debe contar con tecnología de cifrado que preserva el formato FPE para tipos de datos que no son PAN (Primary Account Number).
	El sistema debe permitir la administración de claves heredado para arquitecturas complejas de replicación y escalado.
	El sistema debe soportar un sistema de administración de claves centralizado que coordina la generación y emisión de claves FPE, claves AES y claves IBE.
	El sistema debe administrar las políticas de formato de datos, la aplicación de reglas de negocio sobre el acceso a los datos, la integración con los sistemas de autorización y autenticación de la empresa.
	El sistema debe contar con un servidor de administración de claves que se integre con un servicio autorización y autenticación de la empresa para la asignación de llaves dinámicas.
	El sistema debe poseer herramientas para la generación de scripts para realizar el cifrado masivo y tockenización.
	El sistema debe tener la capacidad de integrarse directamente con la gestión de identidades existente (Active Directory, LDAP y SSO).
	El sistema debe integrarse a sistemas de gestión de eventos e incidentes de seguridad (SIEM).
	El sistema debe tener la capacidad de desidentificar los datos de producción para crear datos estructuralmente válidos para que los desarrolladores puedan realizar un control de calidad o realizar análisis de datos sin exponer datos confidenciales.
	El sistema debe poder revertir de forma segura los datos enmascarados a través de la administración centralizada de claves a su estado original, o hacerlos irreversibles utilizando claves one-time FPE de 256 bits.
	TRANSFERENCIA DE CONOCIMIENTOS
	Se requiere la transferencia de conocimientos técnica para mínimo 6 funcionarios del INEC, sobre la administración de las herramientas utilizada de 20 horas.
	HERRAMIENTA DE ANÁLISIS ESTÁTICO Y DINÁMICO
	El licenciamiento del sistema de Análisis Estático y Dinámico de Aplicaciones debe incluir licenciamiento perpetuo.
	El sistema debe incluir licenciamiento de soporte con fabricante por 2 años

	El sistema debe ser instalado en la infraestructura virtual del INEC.
	El proveedor deberá configurar 10 aplicaciones definidas por el INEC.
	Análisis de seguridad de aplicaciones en esquema virtualizado para un mínimo de 16 aplicaciones desarrolladas internamente por INEC.
	El fabricante deberá estar en el cuadrante de líder en los análisis " Gartner Magic Quadrant" relacionados con application security testing los últimos 5 años.
	El sistema deberá permitir ilimitado número de escaneos para ilimitado número de aplicaciones, proyectos y/o microservicios.
	El sistema deberá permitir ilimitado número de escaneos estáticos y/o dinámicos en modalidad on-premise perpetua.
	El sistema deberá contar con la capacidad de invocar escaneos estáticos y/o dinámicos desde distintas interfaces: CLI, GUI, WEB, plugins y/o uso de APIs
	El sistema deberá contar con la capacidad de integrar sin costo adicional, entrenamiento para desarrollo seguro de aplicaciones en los lenguajes de programación más comunes utilizados por los programadores a través de una plataforma en línea.
	CARACTERÍSTICAS TÉCNICAS DE ANÁLISIS
	Debe mantener la información de auditoría y supresiones de problemas incluso si hay cambios entre cada escaneo realizado. Esto elimina la necesidad de auditar / triangular el mismo 'issue' cada vez que hay un escaneo y permite enfocarse únicamente en los deltas de escaneo
	Debe soportar la ejecución de análisis estático ya sea conectado o desconectado de su repositorio central. Aunque el repositorio central es un componente crítico, aspectos como la latencia de la red (especialmente para las ubicaciones distantes) y la conectividad, no deben ser factores que no permitan realizar el análisis estático
	Debe contar con la capacidad para llevar a cabo el análisis de flujo de datos a través de múltiples lenguajes de programación y/o niveles de aplicación (por ejemplo, JSP a Java a EJB a un procedimiento almacenado de Oracle que corre en uno o más entornos de ejecución).
	Debe soportar el análisis de código fuente mediante línea de comando, integración continua, generador de scripts, integración con IDES (Visual Studio, Android Studio, Jdeveloper, InteliJ, Eclipse) y cluster de escaneo estático.
	Debe tener una alta capacidad de integración con herramientas de build como Maven, Ant, Make, MSBuild, Devenv y Xcode

	Debe integrarse con herramientas de integración continua como Jenkins/Hudson, IBM RTC, Microsoft Team Foundation
	No debe reportar vulnerabilidades en lógica de programación que haya sido comentada, con fin de reducir la tasa de falsos positivos
	Debe soportar la actualización de reglas de 'secure coding' sin que cambie el motor de escaneo de código fuente. Esto permite contar con características mejoradas de análisis, mejor y mayor soporte al análisis de nuevos lenguajes, APIs y tecnologías open source, sin necesidad de actualizar los binarios de la aplicación
	Debe hacer pública una lista detallada de las vulnerabilidades que puede detectar por cada lenguaje de programación soportado
	Debe tener la capacidad de identificar piezas de código malintencionado generado por el desarrollador, sin necesidad de exponer esta capacidad al equipo de desarrollo
	Debe soportar la capacidad de crear reglas personalizadas de análisis de código orientadas a la seguridad, la estandarización del código o a la identificación de patrones de desarrollo a evitar, etc. Todo esto mediante una interfaz gráfica en la que se generan estas reglas que se integran con el analizador de código
	Para las pruebas de seguridad de código fuente en el lenguaje de programación Java, deberá incorporarse la posibilidad de identificar problemas de calidad mediante la herramienta FindBugs
	Para las pruebas de análisis de aplicaciones basadas en el lenguaje de programación Java, deberá soportarse el análisis a nivel bytecode, sin necesidad de contar con el código fuente de la aplicación
	El sistema deberá ofrecer la posibilidad de habilitar el análisis paralelo de proyectos de gran tamaño utilizando múltiples CPUs y cores de un servidor y con optimización automática del uso de memoria, indicando al analizador de código la cantidad de threads a utilizar y la cantidad de memoria reservada para cada thread
	El sistema deber ofrecer la posibilidad de realizar la traducción de código en un equipo de cómputo y el análisis de los modelos traducidos en otro, con el fin de centralizar o distribuir la ejecución de las pruebas de acuerdo con las plataformas de hardware y sistema operativo utilizadas por la organización
	Las descripciones de los problemas identificados, así como las recomendaciones de solución deberán presentarse en idioma español
	El entorno de auditoría de código para especialistas de seguridad deberá ser capaz de detectar y correlacionar problemas reportados provenientes del análisis SAST/DAST/IAST del sistema
	El sistema deberá permitir la creación de reglas personalizadas de

	supresión, para dejar de reportar algún problema identificado como falso positivo por parte del usuario
	El sistema deberá permitir la creación de reglas personalizadas de limpieza de inputs.
	El sistema deberá permitir la definición de métodos seguros utilizados en la validación, limpieza y tratamiento de datos provenientes de fuentes no confiables de información.
	El sistema deberá permitir la implementación de una arquitectura centralizada que permita utilizar los recursos de un pool de servidores para la realización de escaneos.
	CARACTERÍSTICAS DE REVISIÓN Y REMEDIACIÓN
	Debe contar con una robusta integración con los IDEs estándar de la organización para incluir en él la posibilidad de realizar escaneo de código, recuperación remota de resultados de escaneos, remediación de código, descripciones y recomendaciones de buenas prácticas de secure coding y la actualización en el repositorio central de los problemas de seguridad reportados
	Debe soportar el análisis de código fuera o dentro del IDE e independientemente de si la aplicación compila o no
	Debe contar con herramientas que permitan ejecutar escaneos al código fuente sin necesidad de contar con un IDE
	Debe contar con la capacidad de habilitar la colaboración de revisión de resultados, correlación de resultados, auditoría, asignación de problemas y creación de defectos sin necesidad de instalar localmente herramientas propias para estos fines
	Debe permitir la creación de filtros y etiquetas personalizables adaptables al contexto de la organización y sus necesidades de enfoque y priorización. Debe soportar la definición de filtros de forma previa al escaneo (para mejorar el desempeño del análisis) y en etapa posterior al escaneo (para ocultar los problemas que se definan a diferentes audiencias)
	Debe soportar la personalización de visualización de resultados basado en la audiencia (developer, security, etc.)
	Debe permitir la personalización de las descripciones de las vulnerabilidades y las recomendaciones en un Repositorio Central para que haya posibilidad de integrar las descripciones con las políticas internas definidas en la organización, por ejemplo: El INEC podrá personalizar la descripción de determinada vulnerabilidad bajo el contexto de la organización y la aplicación, de forma que más adelante sea posible asociar dichas descripciones a las políticas internas que previamente se han definido.
	Debe ser capaz de llevar un histórico de todos los comentarios y priorizaciones definidos por el usuario

	Debe ser capaz de manejar etiquetas de metadatos que permitan asociar los problemas reportados con las políticas de codificación segura definidas en la organización
	CARACTERÍSTICAS DE ANÁLISIS DINÁMICO
	Capacidad de analizar aplicaciones web, web services basados en REST y SOAP, aplicaciones móviles nativas, sitios web para dispositivos móviles y servicios web del backend de aplicaciones móviles.
	Capacidad de descubrimiento crawling basado en los siguientes métodos: Automatic Crawl-and-Audit, Automatic Crawl-Only, Automatic Audit Only, Workflow-Driven Scan (macro), List-Driven Scan (TXT o XML input) y Restrict-To-Folder
	Posibilidad de analizar aplicaciones de forma calendarizada y en batch, así como capacidad de hacer descubrimiento de aplicaciones web y servicios web en diferentes segmentos de la red interna de la organización.
	Deberá contar sin costo ni licencias adicionales la posibilidad de ejecutar pruebas bajo el modelo de “Interactive Application Security Testing (IAST)”, con el fin de identificar el comportamiento interno y la causa raíz del problema de las aplicaciones que se estén probando. Esta funcionalidad deberá ser propia del fabricante.
	Deberá contar con una API de control y uso remoto basada en servicios RESTful, con el fin de configurar nuevos análisis, recuperar información sobre el estado de los análisis y exportar los resultados de los análisis de forma automatizada
	Las descripciones de los hallazgos y sus recomendaciones de resolución deberán presentarse en idioma español
	Los resultados deberán ser categorizados utilizando la taxonomía Seven Pernicious Kingdoms (7PK) y Common Weakness Enumeration (CWE)
	Capacidad de importar análisis asociados con las herramientas Unified Functional Testing (UFT) (por ejemplo: Burp Suite, Selenium u otras similares) con el fin de tener una amplia cobertura en las pruebas realizadas
	Se deberán soportar los siguientes tipos de autenticación: Network Authentication, Automatic, Basic, Digest, Kerberos, NTLM, Simple, Credentials entered as default Form Entries, Manually inserted cookie/session token, Forms Authentication, Login Macro, Standard reply, Paramaterized inputs, Challenge-Response Questions (Q&A), Certificates, Client-side Certificates, PKI / Token, WS-Security (for SOAP web services), Two-Factor, Interactive Scan (CAPTCHA, RSA ID, Virtual keyboard)
	Deberá permitir detectar automáticamente si una vulnerabilidad previamente detectada fue solucionada o no, sin la necesidad de volver a correr un “escaneo completo" (full scan), así como la importación de falsos positivos generados en escaneos anteriores, antes de la ejecución del

	escaneo o durante la revisión de resultados
	Deberá incluir al menos 20 diferentes políticas de escaneo predefinidas, y permitir la modificación de dichas políticas, además de la generación de políticas de escaneo personalizadas
	Deberá proveer una interfaz gráfica para la modificación manual de la criticidad de las vulnerabilidades.
	Deberá proveer funcionalidad para la generación de reportes de diversos tipos (al menos 15 diferentes tipos), así como un editor de reportes (sin costo adicional) con los cuales sea posible modificar los existentes, extenderlos o crear reportes nuevos
	Deberá contar con al menos 40 plantillas de reportes
	Los resultados de análisis dinámico con tecnologías IAST deberán ser correlacionables con los resultados de las tecnologías de análisis estático de El sistema
	Deberá soportar al menos las siguientes clasificaciones de riesgo: Crítico: Problemas de alto impacto al negocio y con alta probabilidad de ser atacados o ejecutados. Alto: Problemas de alto impacto al negocio y con baja probabilidad de ser atacados o ejecutados. Medio: Problemas de bajo impacto al negocio y con alta probabilidad de ser atacados o ejecutados. Bajo: Problemas de bajo impacto al negocio y con baja probabilidad de ser atacados o ejecutados.
	Deberá soportar al menos las siguientes tecnologías: JavaScript, AJAX, WSDL, SOAP, XML, JSON, Flash, HTML5, Web 2.0, SilverLight y WADL.
	Deberá contar con mecanismos automáticos de actualización tanto en su base de conocimiento, políticas y reglas, así como también en información relevante para el usuario, como nuevas versiones del producto.
	En los reportes que ofrece por default, en caso de no detectar vulnerabilidades, deberá mostrarse un listado detallado de los componentes analizados y no debe generar reportes en blanco o sin contenido
	CARACTERÍSTICAS DE GESTIÓN DE VULNERABILIDADES
	Debe soportar la agregación, normalización priorización y correlación de problemas de seguridad derivados del análisis estático, dinámico e

	interactivo (SAST/DAST/IAST). Debe soportar la integración tanto de resultados identificados de forma automática como de forma manual
	El sistema deberá ofrecer la capacidad de integrarse con el bugtracker Bugzilla
	El sistema deberá ofrecer la capacidad de integrarse con el bugtracker JIRA / TFS
	El sistema deberá ofrecer la capacidad de integrarse con el bugtracker HP ALM
	El sistema deberá incluir el código fuente de los plugins de integración con bugtrackers para que la organización tenga la posibilidad de integrar El sistema con otros bugtrackers no incluidos por default en El sistema
	Debe soportar la capacidad de asignar la revisión y/o remediación de problemas a algún participante de algún proyecto en específico. Debe permitir a un participante de algún proyecto específico el poder visualizar sólo los problemas de seguridad que le fueron asignados
	Debe proveer la capacidad de identificar problemas que fueron ocultados, suprimidos o marcados como "no es un problema" de forma deliberada
	Debe contar con la capacidad de integrar los resultados de los análisis auditados a un repositorio central, así como poder medir los resultados contra diferentes indicadores de rendimiento (KPI) y enviar alertas si alguna política definida por el usuario es violada
	Debe ser capaz de mapear los problemas de seguridad a regulaciones de industria y clasificaciones de problemas conocidos públicamente.
	Debe soportar la generación de reportes específicamente de dichas regulaciones y clasificaciones
	Características de Administración de la Plataforma
	Debe soportar la autenticación via LDAP/AD
	Debe soportar autorización (proyecto y rol) via LDAP/AD
	Debe contar con un repositorio central con el que sea posible y de forma simplificada, automatizada y consistente, la diseminación de folders personalizados, filtros y etiquetas a los visualizadores distribuidos de resultados
	Debe contar con un repositorio central con el que sea posible y de forma simplificada, automatizada y consistente, la diseminación de reglas de codificación segura hacia los usuarios encargados del escaneo de código fuente
	El sistema deberá incluir el código fuente de los plugins de integración con bugtrackers para que la organización tenga la posibilidad de integrar El sistema con otros bugtrackers no incluidos por default en El sistema

	Debe ofrecer la capacidad de automatizar los procesos asociados a las iniciativas de seguridad aplicativa de la organización. Dicha automatización deberá permitir la asignación de tareas, aprobaciones, alertas, reportes, gestión de documentos e inventariado de aplicaciones
	Debe soportar la capacidad de generar a nivel granular, la creación de roles personalizados, para permitir/denegar privilegios de uso en la plataforma de acuerdo con las políticas de seguridad de la organización
	Debe ser capaz de generar reportes de múltiples proyectos / unidades de negocio/ tecnologías con el fin de medir y reportar la efectividad de los esfuerzos de seguridad aplicativa en la organización
	Debe ser capaz de integrarse con plataformas de single sign on
	Debe contar con interfaces de integración basadas en web services para extender las funcionalidades del repositorio central
	TRANSFERENCIA DE CONOCIMIENTOS
	Se requiere la transferencia de conocimientos técnica para mínimo 6 funcionarios del INEC, sobre la administración de las herramientas utilizada de 20 horas.
	Transferencia de conocimiento sobre matrícula de licencias, instalación del plugin, plataforma en general.
	Transferencia de conocimiento sobre la matrícula de 5 aplicaciones en la plataforma.
	CORRELACIONADOR DE EVENTOS
	El sistema de SIEM debe ofrecer un modelo basado en software con una capacidad de >= 1000 EPS, el cual puede tener un crecimiento importante.
	El licenciamiento del sistema SIEM debe ser Perpetuo con licenciamiento a 2 años de soporte con fabricante.
	El sistema debe ser instalada en la infraestructura del INEC en modo virtual
	Deberá tener la capacidad de soportar en forma separada distintos clientes en una única solución (Capacidad multi-tenant).
	Deberá permitir crear nuevos casos de uso (tanto en reglas de correlación, reportes y dashboard)
	Debe permitir organizar y clasificar a los activos monitoreados bajo categorías independientes y personalizables, permitiendo y favoreciendo su utilización en filtros, monitores gráficos, reglas de correlación, entre otros para eliminación de falsos positivos. Ejemplos de categorías para la clasificación de activos: - Nivel de Criticidad - Función dentro de la organización

	- Aplicativo residente - Nivel de seguridad de la Información Almacenada - Nivel de Acceso
	Deberá soportar la definición de listas de observación estáticas y dinámicas (listas blancas, negras, sospechosos, hostiles, de exclusión) que puedan ser actualizadas y consultadas de forma automática en el proceso de correlación en tiempo real, para identificar ataques o atacantes recurrentes, escalamiento de amenazas persistentes, entre otros. Estas listas deben soportar más de 2 campos como mínimo.
	Deberá soportar la definición de listas de sesión de usuarios en adición a las listas de observación. Las listas de sesión tendrán la capacidad de mantener un registro detallado de inicio y cierre que puedan ser utilizadas en la correlación de eventos y dispositivos orientados a sesión como VPN, DHCP, Active Directory, etc.
	Deberá permitir modelar y configurar las distintas redes, con la capacidad de diferenciar redes con traslape (overlapping), zonas y recursos monitoreados, que puedan ser cargados a partir de una lista de activos generada por plataformas de gestión de configuraciones (CMDB).
	El proveedor debe integrar 20 activos designados por el INEC.
	De igual forma El sistema deberá permitir insertar anotaciones de texto libre sobre los eventos base, ya sea de manera individual o colectiva, lo cual facilitará identificar qué eventos ya han pasado por un proceso de validación y análisis. Por ejemplo, insertar anotación a todos los eventos que se han reportado durante una ventana de mantenimiento
	Deberá tener la capacidad de colección de correlación 1000 EPS sostenidos.
	El proveedor debe garantizar el uso de conexiones cifradas desde y hacia la red corporativa del INEC
	Características técnicas de Análisis
	El sistema deberá almacenar sus datos en una solución interna de BigData, no se aceptará bases de datos relacionales
	Al tratarse de una solución de seguridad, no debe permitir bajo ningún concepto eliminar eventos ni datos recibidos
	El sistema debe ser capaz de ofrecerse en su totalidad como software, eso incluye, máquinas virtuales.
	El sistema deberá disponer de un sitio web en donde se pueda descargar casos de uso adicionales ya armados. Estos casos de uso deben ser posible modificarlos a gusto.
	Deberá tener una arquitectura modular, es decir con componentes dedicados para la colección y procesamiento de eventos independientes del motor de correlación.

	Deberá estar clasificada como Líder dentro del reporte denominado Cuadrante Mágico de Gartner para tecnologías SIEM publicado, al menos, en los últimos 5 años.
	El sistema deberá ser nueva en su totalidad, con las últimas versiones de software liberadas por el fabricante
	Deberá permitir escalar el licenciamiento a través del incremento de capacidades
	El licenciamiento no debe tener restricciones de cantidad de dispositivos, de dispositivos de red, usuarios ni consolas.
	El sistema deberá incluir sin costo la capacidad de desplegar un componente que haga las funciones de bróker de eventos (mínimo un bróker) para de forma centralizada normalizar, proteger y enriquecer los logs antes de enviarlos hacia los componentes de SIEM, gestión de logs y/o cualquier otro componente.
	El sistema debe permitir que los conectores envíen información a distintos destinos, en distintos formatos, en forma simultánea
	Deberá tener la capacidad de incorporar campos personalizados, además de los que ya trae la normalización, sin afectar considerablemente el storage.
	Los componentes que realizan la recolección de datos (conectores) deberán enviar los eventos hacia el SIEM a través del protocolo de transporte TCP y con técnicas de cifrado y autenticación SSL (Secure Sockets Layer). No se permite el uso de protocolo Syslog/Syslog-ng TCP ni UDP para el envío de eventos de conectores hacia el SIEM.
	Los conectores de eventos remotos o distribuidos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia el SIEM, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos.
	Los conectores de eventos deberán enriquecer mediante categorías los eventos obtenidos en los componentes de recolección a fin de permitir la comprensión y el significado del evento, sin la necesidad de tener conocimiento previo de la bitácora, las categorías requeridas son: - Objeto referido en el evento (Aplicación, Usuario, etc.). - Comportamiento sobre dicho evento (Acceso, Ejecución, Autenticación, etc.). - Resultado de dicha acción (Intento, Éxito, Fallido). - Técnica utilizada - Importancia del evento - Grupo o familia del dispositivo (IDS, Sistema Operativo, etc.)
	El sistema de correlación debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes: - Archivos de logs (bitácoras) con campos delimitados - Archivos de logs (bitácoras) de longitud variable (no delimitados).

	- Bases de datos relacionales por conexión ODBC - Bases de datos relacionales por conexión JDBC - Traps de protocolo SNMP - Eventos enviados por protocolo Syslog - Archivos con formato XML
	El sistema debe incluir un wizard para integrar las fuentes no soportadas en forma nativa, tales como los desarrollos hechos en casa, al menos, para los orígenes de datos más sencillos
	Los componentes que realizan la recolección de eventos deberán realizar desde el origen la normalización completa de los eventos, es decir únicamente enviarán hacia el SIEM los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporteo de los eventos. No se acepta la normalización en un dispositivo que no esté encargado de recolectar
	Los componentes que realizan la recolección de eventos podrán bajo demanda preservar el campo en crudo (raw data) en adición al evento previamente normalizado.
	Los componentes que realizan la recolección de eventos deberán tener la capacidad de generar una firma/hash o huella digital sobre los eventos crudos mediante el uso de algoritmos criptográficos de una sola vía, así mismo los conectores deberán tener la capacidad de validar la integridad de estos eventos.
	Los componentes que realizan la recolección de eventos deberán utilizar el protocolo TCP como medio de transporte hacia El sistema de correlación, verificando constantemente el estado de la conexión por medio de un pulso o “Heartbeat”. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.
	Los componentes que realizan la recolección de eventos podrán agregar etiquetas en campos adicionales sobre los eventos con información proveniente de la configuración y modelado de la red definida en el motor de correlación tales como información de la red, ubicación geográfica, unidad de negocio, que favorezca y optimice el proceso de correlación de eventos.
	Los componentes que realizan la recolección de eventos deberán tener funciones para alcanzar un destino redundante así cuando el destino primario no esté disponible el dispositivo de recolección automáticamente iniciara el envío de los datos al destino secundario. Esta función se refiere únicamente al recolector
	Los componentes que realizan la recolección de eventos deberán tener la capacidad de enviar los datos a múltiples destinos primarios de forma simultánea. Los destinos primarios deberán incluir también destinos de herramientas externas, que no sean de la misma marca del producto, por medio de formato CEF. Esta función excluye escenarios de alta disponibilidad y de failover.

	La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación deberán utilizar mecanismos de compresión de datos. La agregación de datos no se considera similar a la compresión de los datos.
	El sistema debe permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato. Esto no debe ser realizado con tecnología VPN. Favor mostrar explícitamente la documentación donde se menciona esta funcionalidad
	El sistema deber permitir configurar el retraso voluntario en el envío de eventos al motor de correlación basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad.
	El sistema propuesto deberá tener la capacidad de agregación opcional y selectiva de eventos similares basada en campos (más de un campo) definidos por el usuario y bajo una ventana de tiempo parametrizable, enviando al motor de correlación eventos de tipo agregación que contienen la cuenta de eventos previamente agregados en conformidad a la publicación NIST 800-92.
	Los componentes que realizan la recolección de eventos deberán tener la capacidad de filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación en conformidad a la publicación NIST 800-92. Se reitera que esta capacidad de filtrado es a nivel de colección, no de búsqueda.
	Los componentes que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor de NTP. Simplemente almacenar distintos timestamp no se considerará corrección de horario.
	Los componentes que realizan la recolección de eventos deberán ofrecer la capacidad de ofuscar campos sensibles por la sustitución de algoritmos criptográficos de una sola vía (hash).
	Los componentes que realizan la recolección de eventos tendrán la capacidad de administración y actualización remota, sin la necesidad de realizar cambios, ajustes o actualizaciones directamente en el componente.
	Los componentes que realizan la recolección de eventos deberán contar con múltiples perfiles de configuración, los cuales entrarán en funcionamiento en función de horarios preestablecidos.

	El sistema deberá operar con los métodos nativos de auditoría, logs y eventos de cada plataforma/dispositivo/aplicación. Esta recolección debe ser no invasiva, y no debe implicar instalar agentes en todos los equipos. No se aceptará por ningún motivo técnicas de interpretación de tráfico, debido a su conocido problema de pérdida de datos en reconstrucción de sesiones.
	El software de conectores deberá ser soportado para su instalación en plataformas virtuales y deberá considerar cualquier tipo de licencia adicional.
	Todos los conectores deben ser construidos por la misma marca que el resto de los productos, que incluyan normalización en la etapa de colección.
	Todos los conectores deben trabajar con la normalización y categorización de los eventos recibidos. Ambos procesos deben ocurrir en la recolección, y no se aceptará interpretar etiquetas como si fuesen categorías.
	Los conectores deberán ser los encargados de realizar normalización antes de enviar los datos a otros componentes (pudiendo ser uno o más componentes desde un único conector) Las reglas de correlación deben poder construir en forma gráfica, en donde se puede seleccionar los campos obtenidos en la normalización y unirlos por medio de conectores lógicos. En ningún caso se interpretará búsquedas de datos como si fuesen reglas de correlación.
	El sistema de correlación de eventos ofrecida deberá ser integrable “fuera de la caja” (out-of-the-box) como mínimo con más de 350 dispositivos y aplicaciones de más de 100 fabricantes lo cual evitará tener personal dedicado a la modificación de los formatos de logs, mediante componentes denominados conectores/colectores.
	Deberá ser compatible con el estándar libre para la administración y formato común de eventos ofreciendo más de 400 campos para la normalización y distribución de los distintos campos obtenidos a partir de los eventos recolectados (formato CEF)
	Deberá soportar la capacidad integración en forma nativa con los siguientes aplicativos como origen de datos • RSA Aveksa • Bay Dynamics Risk Fabric • BeyondTrust PowerBroker • Cisco Secure Access Control Server (ACS) • CyberArk Privileged Account Security Management (PIM) Suite • CyberArk Privileged Threat Analytics (PTA) • Dell ChangeAuditor DB (Quest) • IBM Tivoli Access Manager • Lieberman ERPM • Netwrix Auditor • Novell Nsure Audit • ObserveIT Enterprise • Oracle Sun ONE Directory Server • VMware® PacketMotion PacketSentry • RSA Authentication Manager • Securonix RTI-Risk and Threat Intelligence • SpectorSoft Spector 360 Export Service • Thycotic Secret Server
	El sistema deberá tener la capacidad de integración, en forma nativa, con Office365 (incluyendo Azure AD, Sharepoint y Exchange).

	El sistema deberá incluir licencia permanente, en ningún caso anual.
	El sistema otorgará la libertad de escoger la integración, en forma nativa, con las siguientes herramientas de análisis de vulnerabilidades. En ningún caso se aceptará herramientas de análisis de vulnerabilidades como parte de la misma herramienta SIEM. • McAfee Vulnerability Manager (FoundScan) • Nmap • Open Vulnerability and Assessment Language (OVAL) Standard • Rapid 7 Nexpose • SOC Prime Integration Framework • Tenable Nessus • SAINT Vulnerability Scanner
	El sistema otorgará la libertad de escoger la integración, en forma nativa, con las siguientes herramientas de análisis de red. En ningún caso se aceptará herramientas de captura de tráfico como parte vital de la misma herramienta SIEM.• Cisco NetFlow/Flexible NetFlow• NetScout nGenius• FireEye nPulse Hammerhead• QoSient Argus• InMon sFlow®• Blue Coat Solera Networks DeepSee• TCPdump
	El sistema otorgará la libertad de escoger la integración, en forma nativa o mediante syslog, con las siguientes herramientas de monitoreo de integridad de archivos/bases de datos. En ningún caso se aceptará herramientas de monitoreo de integridad de archivos/bases de datos como parte vital de la misma herramienta SIEM. • Networker Datadomain, AVAMAR
	El sistema otorgará la libertad de escoger la integración, en forma nativa, con las siguientes herramientas análisis forense de red. • Narus nSystem • NIKSUN NetDetector • RSA NetWitness • General Dynamics (Fidelis) Cybersecurity CIRT
	CARACTERÍSTICAS TÉCNICAS DE ALMACENAMIENTO
	Deberá soportar un almacenamiento para la retención en línea de eventos máximo de 12 TB.
	Deberá permitir definir múltiples grupos de almacenamiento de eventos, con lo cual se podrán crear múltiples repositorios independientes para distintos tipos o fuentes de eventos.
	Deberá permitir políticas de retención de eventos basadas en tamaño (GB) o tiempo (Días), las cuales aplicarán de forma independiente a cada grupo de almacenamiento de eventos, lo que permitirá contar con un almacenamiento de eventos inteligente y auto administrado.
	Deberá contar con un único repositorio para el almacenamiento de todos los eventos enviados y normalizados desde su origen por los conectores, éste repositorio deberá guardar en su totalidad los distintos elementos de cada evento en campos específicos independiente del tipo de dispositivo o aplicativo que la genere, permitiendo así la definición de contenido de correlación entre distintos tipos de dispositivos (firewalls, IDPs, Sistemas Operativos, conocido como cross device correlation) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de datos.

	Deberá ofrecer la capacidad de archivar eventos a un almacenamiento fuera de línea, complementando y aumentando la capacidad total de retención, estos archivos de eventos podrán ser reactivados bajo demanda para poder realizar búsquedas y correlación histórica de eventos
	Las reglas de correlación deben poder construir en forma gráfica (asistente/wizard), en donde se puede seleccionar los campos obtenidos en la normalización y unirlos por medio de conectores lógicos. En ningún caso se interpretará búsquedas de datos como si fuesen reglas de correlación.
	CARACTERÍSTICAS TÉCNICAS DE CORRELACIÓN
	El sistema debe permitir crear cuantas reglas de correlación se necesite. En caso de modificación de reglas de correlación, se necesita que sea en forma gráfica (asistente/wizard). En ningún caso se aceptará la necesidad de modificar consultas de búsquedas de datos como si fuesen reglas de correlación.
	Deberá proporcionar la capacidad de correlación basada en reglas (rule-based) y sin reglas (rule-less) ambas operando de manera concurrente sin adicionar software o equipamiento adicional. Las reglas podrán detectar eventos sobre un solo tipo de eventos así como poder correlacionar eventos entre distintos tipos de eventos.
	Deberá ser capaz de realizar la correlación en tiempo real y en memoria (sobre el flujo entrante de eventos), así como correlación histórica para eventos que han sido colectados fuera de línea (batch). Ambos mecanismos deberán operar de manera concurrente y bajo la misma solución, esto es correlación en tiempo real y correlación histórica en un solo correlacionador. No se aceptará que sobrepasada la cantidad de EPS licenciados exista una especie de encolamiento de eventos, pues se perdería la capacidad de tiempo real.
	El motor de correlación deberá realizar el proceso de análisis de eventos en memoria, es decir, previo a que sean persistidos a la base de datos. No se aceptará la capacidad de almacenar primero los eventos, para posteriormente correlacionar, debido al delay que esto generaría.
	Deberá realizar correlación geo-espacial, es decir, utilizando las direcciones IP de Internet del evento o información de la ubicación del dispositivo para la configuración de reglas para alertas de eventos relacionados y que ocurran en distintas zonas. Ej. El Usuario X realizando intentos de login en dos (02) localidades distintas de forma concurrente.
	Deberá permitir definir ubicaciones físicas o lógicas internas, a las cuales se les podrán asignar coordenadas (latitud, longitud) que permitan identificar la ubicación geo-espacial de origen y destino de los eventos aún y cuando se encuentren bajo segmentos privados de direcciones IP.

	Deberá realizar correlación en tres (03) Dimensiones teniendo la habilidad de unificar y correlacionar eventos, información proveniente de herramientas de análisis de vulnerabilidades y criticidad de los activos o dispositivos que permita eliminar falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando los factores mencionados.
	Deberá tener la capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos, tales como realizar el cálculo de algún valor (ej.: sumar o restar, redondear) o derivar algún dato particular (ej.: día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (ej. Generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del día).
	Deberá tener la capacidad de detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio, desviación estándar, curtosis, varianza. Así mismo estos comportamientos podrán ser graficados para su análisis en tiempo real.
	Deberá permitir probar reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previo a su despliegue en monitoreo en tiempo real. Esta funcionalidad permitirá reducir los falsos positivos y falsos negativos.
	Deberá permitir integrar en el proceso de análisis en tiempo real los eventos previamente generados por el motor de correlación, es decir, adicional a los eventos base recibidos por los colectores de eventos, analizar los eventos de correlación previamente identificados, a fin de identificar amenazas o patrones más complejos.
	Deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación sin la necesidad de integrar software o equipamiento adicional - Importancia del evento - Criticidad del activo - Vulnerabilidades asociadas - Antecedentes previos sobre el origen, destino o ambos.
	Las reglas de correlación deberán tener la capacidad como respuesta automática ante una regla de correlación activada la ejecución de un script o comando a nivel sistema operativo con la capacidad de poder enviar parámetros que sean derivados a partir de los eventos asociados. Los comandos deberán ser ejecutados desde el mismo correlacionador ya sea de manera autónoma o bien mediante confirmación en consola o también directamente en los componentes que recolectan los eventos.
	Deberá ser capaz de enviar alertas vía email, traps SNMPv1, SNMPv2 y SNMPv3 así como notificaciones directo a la consola de administración.
	Deberá tener la capacidad de crear casos de forma automatizada e incluso de alimentar casos (tickets) ya existentes como mecanismos de acción de las reglas de correlación.

	Contar con la capacidad de limitar bajo qué condiciones una regla ejecutará una o más acciones, evitando así generar múltiples acciones ante eventos repetitivos, pudiendo controlar el flujo de acciones y notificaciones: - Acción solo bajo el primer evento o umbral alcanzado. - Acción bajo eventos o umbrales subsecuentes (descartar el primero). - Acción en cada evento o umbral alcanzado. - Bajo una ventana de tiempo específica.
	El sistema deberá tener la capacidad de ejecutar reglas de correlación en tiempo real, corriendo constantemente en memoria. No se aceptará solamente reglas ejecutándose en periodos.
	El sistema debe permitir que las alertas de las reglas de correlación envíen información a distintos destinos, en distintos formatos, en forma simultánea
	CARACTERÍSTICAS DE LA INTERFAZ GRÁFICA DE ADMINISTRACIÓN
	Deberá ofrecer al menos una interfaz de administración, la cual permitirá administrar los recursos de El sistema, así como permitir visualizar el estado de la seguridad, dashboards, ejecutar reportes.
	Deberá utilizar y mostrar los eventos recolectados de forma estructurada, es decir deberán ser previamente analizados y normalizados en su totalidad y distribuidos en los campos específicos con el fin de permitir y facilitar el análisis de eventos incluso de múltiples tipos de dispositivos.
	Deberá tener la capacidad de realizar búsquedas sobre los eventos almacenados ya sea a través de palabras clave (keywords), campos específicos o bien una combinación de ambas. Estas búsquedas podrán ser ingresadas en formato libre a través de un cuadro de texto.
	Deberá asistir en el momento de ingresar manualmente la cadena de búsqueda, reduciendo el tiempo requerido para generar búsquedas y explotar eventos, a través del despliegue de las siguientes ayudas: • Histórico de búsquedas. • Operadores recientemente utilizados • Ejemplos de utilización de operadores • Sugerencia de operadores de búsqueda • Listado de campos disponibles • Listado de operadores disponibles
	Deberá ser capaz de profundizar en los resultados previamente obtenidos de las búsquedas en texto libre complementándolo con operadores adicionales de búsqueda, los cuales extraerán información de interés permitiendo obtener información como el top N de eventos, promedio (avg), ordenar (sort), últimos N eventos (tail).

	La interfaz de administración gráfica deberá permitir la importación de gráficos a manera de diagramas que permitan asociar tableros gráficos visuales (dashboards) a una determinada porción o segmento del diagrama para proveer de una visualización lógica y estado situacional de la seguridad en determinada zona de la red o negocio.
	La interfaz de administración gráfica deberá tener la capacidad de graficar la ruta y comportamiento de un conjunto de eventos a través del uso de nodos, de tal forma que sea posible generar una abstracción visual de los mismos que incluya como mínimo las siguientes vistas: - Jerárquica – Orgánica - Circular
	La Interfaz de administración gráfica deberá ofrecer herramientas integradas que permitan analizar la información proveniente de tableros gráficos (dashboards) con la capacidad de profundizar para identificar la causa raíz (drill-down).
	La interfaz de administración gráfica deberá desplegar los eventos de correlación, así como el evento o eventos base relacionados, pudiendo ver la cadena de eventos bajo la misma vista.
	La interfaz de administración gráfica deberá permitir generar una base de conocimiento (KB) a través de las cuales se pueda generar y consultar información, protocolos a seguir y asociarlos a eventos, casos, reportes. Este conocimiento generado estará disponible para analistas y operadores.
	El sistema debe permitir llegar a más detalles (realizar drill-down) sin necesidad de acceder a otras interfaces/clientes distintas.
	Deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: - PDF - CSV – HTML - RTF
	CONSIDERACIONES DEL PROVEEDOR
	Presentar un plan de comunicación y escalamiento que asegure la comunicación entre sus áreas comerciales y operativas y personal del INEC
	Contar suscripciones a CERT o CSIRT ecuatoriano e internacionales, grupos de respuesta a incidentes de seguridad informática.
	El proveedor deberá contar con al menos una certificación vigente y actualizada como ISO27001:2013, ISO9001:2015, ISO 20000:2011, que ayuden a gestionar adecuadamente el servicio y el manejo de la seguridad de la información del INEC y que estén relacionadas con el servicio.
	TRANSFERENCIA DE CONOCIMIENTOS
	Transferencia de conocimientos técnica para mínimo 6 funcionarios del INEC, sobre la administración de las herramientas utilizadas de 20 horas.
	• El proveedor será responsable de la instalación y configuración de todos los componentes de las licencias adquiridas. • El proveedor ejecutará las pruebas de funcionamiento y afinamiento

	de todo el licenciamiento ofertado. • El proveedor elaborará las memorias técnicas (documentación) de instalación, configuración, diagramas (si aplica) y puesta en producción de las licencias ofertadas. • Se requerirán los manuales técnicos que prevean de uso, operación y mantenimiento, los que deberán encontrarse en idioma español y cuya entrega se efectuará conjuntamente con las licencias suministradas al momento de la recepción del proyecto. Los manuales de usuario y técnicos pueden ser entregados en medios digitales. El juego de manuales estará integrado por: o Manual de Uso y Operación: con instrucciones de manejo y cuidados a tener en cuenta para la licencia; y, o Manual de Servicio Técnico: con información detallada para su instalación, funcionamiento, entre otros. • El oferente deberá realizar la ejecución del proyecto en 30 días calendario.
Tipo de Compra	Servicio
Comprenderá negociación	Sí, de conformidad con la normativa (art 47 del RGLOSNCP), de ser el caso.
Fecha límite para receptar solicitudes	De conformidad a lo establecido en los pliegos del procedimiento de contratación
Dirección para presentación de ofertas	Las ofertas deben ser presentadas conforme con las disposiciones y directrices del Servicio Nacional de Contratación Pública en la cual en el artículo 74 del nuevo RLOSNCP indica: "La oferta se deberá presentar únicamente a través del Portal COMPRASPÚBLICAS hasta la fecha límite para su presentación, debidamente firmada electrónicamente..."y también conforme el artículo 32 del mismo reglamento y demás normativa pertinente.
Idioma de Presentación de Ofertas	Español
Condiciones para la participación de los proveedores	De conformidad con lo establecido en el pliego del procedimiento de contratación.

Firmado electrónicamente por:
SANDRA JACQUELINE RUNDO ACURIO

Ing. Sandra Jacqueline Rundo Acurio
COORDINADORA GENERAL ADMINISTRADORA FINANCIERA
INSTITUTO NACIONAL DE ESTADISTICAS Y CENSOS.