INFORME DEL COMITÉ DE EVALUACIÓN Nº 69 / 2015
LICITACIÓN POR CONCURSO DE OFERTAS Nº 15/2015
"ADQUISICIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y GESTIÓN DE EVENTOS (SIEM)"
ID 298820

1. Introducción

En fecha 20 de octubre, este Comité se ha abocado a la elaboración del presente informe, con posterioridad al estudio de las ofertas presentadas para el llamado a Licitación por Concurso de Ofertas Nº 18/2015, de acuerdo con las especificaciones técnicas y demás documentos inherentes al presente procedimiento de contratación, a fin de determinar la oferta más conveniente para los intereses de la Dirección Nacional de Contrataciones Públicas.

2. Antecedentes

a) **Nº de PAC:** ID 298820

b) **Aprobación:** se cuenta con la aprobación del Director Nacional, mediante Resolución DNCP Nº 2687/2015, de fecha 10 de setiembre de 2015 para el inicio del procedimiento de contratación.

c) **Disponibilidad Presupuestaria:** la cobertura presupuestaria para la obligación y pago, se encuentra en el rubro 570, FF30 del ejercicio fiscal 2015. Por tratarse de una contratación plurianual, la partida arancelaria del 2016 se encuentra sujeta a su aprobación.

d) **Publicación:**
- En el SICP 18/09/2015

e) Se ha cursado invitaciones a las siguientes empresas: ONE S.A., LOGICALIS S.A., STARK TECNOLOGIA S.A., TECHNOMA SOCIEDAD ANONIMA COMERCIAL E INDUSTRIAL y NEXSYS DE PARAGUAY S.A.

f) **Miembros del Comité de Evaluación:** han sido designados, el Sr. Fernando Caballero, la Lic. Noelia Ricagno, y el Abg. Humberto Báez, que evaluarán y recomendarán la adjudicación de las ofertas que estimen más solventes y convenientes.

3. Acto de Apertura

De acuerdo al procedimiento previsto por el Articulo 54 *"Acto de apertura..."* del Decreto Reglamentario Nº 21909/03 y concordantes, se ha llevado a cabo el Acto de Apertura de Sobres y verificación de Ofertas, en el local de la Dirección Nacional de Contrataciones Públicas, sito en la Calle Estados Unidos Nº 961 c/ Teniente Fariña de la ciudad de Asunción, en fecha 12 de octubre del corriente, contando con la presentación de 1 (una) oferta, perteneciente a la firma **STARK TECNOLOGIA S.A.**

4. Precios ofertados

Ítem	Bien	Cant.	STARK TECNOLOGIA S.A.
			Precio Total - (IVA incluido)
1	Sistema de Información de Seguridad y Gestión de Eventos (SIEM)	1	395.000.000
TOTAL			**395.000.000**

5. Análisis de las ofertas y verificación de la Documentación Presentada

A fin de determinar el cumplimiento de los requisitos establecidos en el Pliego de Bases y Condiciones, basado en las especificaciones técnicas se pasa a verificar el cumplimiento de la misma en la siguiente planilla:

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

ESPECIFICACIONES TÉCNICAS			STARK TECNOLOGÍA S.A.	
Sistema de Información de Seguridad y Gestión de Eventos (SIEM)				
Características		Mínimo Exigido	Cumple con las especificaciones requeridas (sí / no)	Observaciones Oferta adicional a especificaciones técnicas
Cantidad requerida	1 (uno)	Exigido	SI	
Factor de forma	Appliance ó Virtual	Exigido	SI	
Capacidad mínima requerida de EPS	1.000	Exigido	SI	
Capacidad mínima de FPM	15.000	Exigido	SI	
Gestión Administrativa	La solución SIEM debe proporcionar una gestión centralizada de todos los componentes y funciones administrativas desde una única interfaz basada en web.	Exigido	SI	
	La solución debe definir el acceso basado en roles, por dispositivo, grupo de dispositivos, rangos de red. También debe restringir a los usuarios y/o grupos acceso solo a la información de dispositivos, grupos de dispositivos y rangos de red respectivos. Esto incluye ser capaz de restringir el acceso de un usuario a funciones específicas de la solución que no está dentro del alcance de un papel usuarios incluyendo, pero no limitados a, la administración, presentación de informes, el filtrado de eventos, de correlación, y / o la visualización de Dashboard.	Exigido	SI	
	La solución debe realizar el discovery en forma automática de los activos que están siendo protegidos o monitoreados. Debe realizar la clasificación automática de los mismos.	Exigido	SI	
	La solución debe contar con una interfaz de trabajo (Dashboard) totalmente configurable y customizable acorde a las diferentes áreas de la DTI.	Exigido	SI	
	La solución debe proveer los mecanismos para la encriptación de la comunicación entre los componentes.	Exigido	SI	
	Debe poder integrarse con sistemas de Directorios como método de autenticación, como mínimo Active Directory, LDAP, Radius, TACAS.	Exigido	SI	
	La solución debe proveer una API para el acceso a los datos almacenados en la Base de Datos.	Exigido	SI	
Prestaciones a nivel operativo	La solución debe poseer una interfaz gráfica de usuario basada en web para la gestión, el análisis y presentación de informes.	Exigido	SI	
	La solución debe ser compatible con la actualización automática de la información de configuración con una intervención mínima del usuario. Por ejemplo, las actualizaciones de seguridad, actualizaciones de la taxonomía de reglas proveedor, soporte de dispositivos.	Exigido	SI	

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe contar con un proceso de copia de seguridad / recuperación automatizada. Debe realizar la compresión de datos ante falta de espacio en disco y realizar el archivado en forma selectiva (gestionar la retención de distintos tipos de eventos dependiendo de su criticidad).	Exigido	SI	
	Debe asegurar que todos los componentes de sistemas distribuidos continúan funcionando cuando cualquier otra parte del sistema falla o pierde la conectividad. Es decir, la consola de administración pudiera estar fuera de línea, todos los colectores separados todavía continúan trabajando en la captura de registros, que se actualizarán al restablecimiento de la comunicación.	Exigido	SI	
	La solución debe soportar la configuración de alta disponibilidad en un modo integrado y sin la necesidad de software de 3 ª parte adicional.	Exigido	SI	
	Debe asegurar que todos los componentes de sistemas distribuidos continúan funcionando cuando cualquier otra parte del sistema falla o pierde la conectividad. Es decir, la consola de administración pudiera estar fuera de línea, todos los colectores separados todavía continúan trabajando en la captura de registros, que se actualizarán al restablecimiento de la comunicación.	Exigido	SI	
	La solución debe poder crecer en el agregado de la funcionalidad de Gestión de Vulnerabilidades, sin que ello represente la introducción de soluciones de terceros, y deberán ser gestionadas desde la misma consola web del SIEM. El oferente deberá indicar el nombre del módulo funcional que cumplirá con este requerimiento.	Exigido	SI	IBM Security Qradar Vulnerability Manager
	La solución debe poder crecer en el agregado de la funcionalidad de Gestión de Riesgos, sin que ello represente la introducción de soluciones de terceros, y deberán ser gestionadas desde la misma consola web del SIEM. El oferente deberá indicar el nombre del módulo funcional que cumplirá con este requerimiento.	Exigido	SI	IBM Security Qradar Risk Manager
	Debe realizar la supresión de eventos, así poder manejar situaciones de event storm.	Exigido	SI	
	La solución debe permitir implementaciones como software y / o appliance.	Exigido	SI	
	La solución debe ofrecer widgets del Dashboard personalizables que pueden presentar información de seguridad relevante para los usuarios del sistema (es decir, puntos de vista de eventos, vistas de actividad de red, puntos de vista de incidentes, etc.).	Exigido	SI	
	La solución debe en forma automática realizar Health Check y notificar en el caso de que se detecte algún inconveniente.	Exigido	SI	

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe ser capaz de mantener una base de datos de todos los activos descubiertos en la red. Estos datos de activos deben incluir información importante sobre el activo y de la información recogida (es decir, los atributos del sistema, los atributos de red, estado de vulnerabilidad, riesgos asociados, etc.) La base de datos debe ofrecer la posibilidad de editar los atributos cuando no se pueden descubrir en forma automática (es decir, departamento, ubicación, etc.) El usuario debe ser capaz realizar búsquedas en esta base de datos.	Exigido	SI	
	Análisis de sesiones de red (Layer 7).	Exigido	SI	
	Debe analizar e identificar direcciones IP y poder verificar la reputación de la misma, con el fin de detectar direcciones sospechosas y enriquecer el análisis de los eventos. Esta lista de reputaciones de dirección IP debe ser actualizado en forma automática y periódica por el fabricante. Por ejemplo: detectar puntos de distribución de malware, comandos botnet, proxys anónimos, servidores de spam.	Exigido	SI	
	La solución debe proveer Dashboard Out-of-thebox, a fin de que ayude a los administradores a una mejor visión de la información. Por ejemplo, Dashboard de compliances, de vulnerabilidades, de log activity entre otros.	Exigido	SI	
Análisis y Filtrado de Eventos	La solución debe realizar un análisis en tiempo real de los eventos.	Exigido	SI	
	La solución debe realizar el Drill-down avanzado de eventos en caso de ser necesario y esta podrá ser realizada desde los gráficos y dashboard.	Exigido	SI	
	La solución, debe poder agregar y analizar eventos basados en filtros específicos realizados por el usuario.	Exigido	SI	
	La solución debe generar alertas sobre la base de análisis de anomalías observadas y los cambios de comportamiento en los eventos de la red y de seguridad.	Exigido	SI	
	La solución debe realizar correlación de eventos dentro de una misma alerta.	Exigido	SI	
	La solución debe contextualizar vulnerabilidades dentro de la correlación.	Exigido	SI	
	La solución debe realizar correlación de eventos históricos, que permita correr eventos pasados por las nuevas reglas creadas, a fin de poder recrear ofensas y detectar comportamiento malicioso.	Exigido	SI	
	La solución debe proporcionar una vista streaming en tiempo real que soporte las capacidades de filtrado completo.	Exigido	SI	
	La solución debe realizar análisis de tendencias a largo plazo de los eventos.	Exigido	SI	
	La solución debe apoyar y mantener un historial de la actividad de autenticación de usuario en función de cada activo.	Exigido	SI	
Correlacionador SIEM	La solución debe vigilar y alertar cuando hay una interrupción en la recopilación de registros de un dispositivo. En otras palabras, si los registros no son vistos desde un servidor en minutos X a continuación, generar una alerta.	Exigido	SI	

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe proporcionar la capacidad de transmitir alertas usando múltiples protocolos y mecanismos a otras soluciones de gestión.	Exigido	SI	
	La solución debe proporcionar la capacidad de correlacionar la información a través de dispositivos potencialmente dispares.	Exigido	SI	
	La solución debe proporcionar alertas en base a las amenazas de seguridad observados en los dispositivos monitoreados.	Exigido	SI	
	La solución debe proporcionar alertas en base a la política establecida. (Por ejemplo, no se permite el tráfico de protocolos p2p.)	Exigido	SI	
	La solución debe generar alertas basados en pesos, para tener en cuenta las prioridades. Los pesos deben poder asignarse sobre la base de múltiples características, como el tipo de activos, el protocolo, la aplicación.	Exigido	SI	
	La solución debe proporcionar alertas sobre la base de las anomalías observadas y los cambios de comportamiento en la actividad de red de datos (flow)	Exigido	SI	
	La solución debe realizar la correlación de valores aditivos a través del tiempo. Por ejemplo, alerta cuando cualquier IP SRC envía más de 1 GB de datos a un solo puerto en una sola DST IP en un periodo de una hora de tiempo.	Exigido	SI	
	La solución debe poseerla capacidad de correlacionar eventos, contra información de productos de seguridad terceros (es decir, la cartografía redes de botnets conocidos hostiles conocidos, etc.) Estas fuentes de datos de terceros deben ser actualizados automáticamente por la solución.	Exigido	SI	
	La solución debe realizar la correlación de una secuencia fallida. Ejemplo un servicio parado, que no fue seguido del restablecimiento normal del servicio luego de 5 minutos.	Exigido	SI	
	La solución debe proporcionar un mecanismo out-of-the-box para descubrir y clasificar los activos por tipo de perfiles (es decir, servidores de correo frente a servidores de bases de datos) para minimizar los falsos positivos asociados a una mala clasificación de los activos.	Exigido	SI	
	La solución debe limitar la presentación de múltiples alertas similares.	Exigido	SI	
	La solución debe proporcionar un mecanismo, para optimizar el tunning de las reglas, que permite la agrupación de valores de entrada similares de una regla de correlación que puede ser utilizado por varias reglas. Este mecanismo de agrupación deberá permitir tanto para grupos estáticos, como grupos dinámicos creados por otras reglas de correlación. Por ejemplo, el usuario del sistema puede definir un grupo de puertos / protocolos prohibidos que se debe utilizar a través de múltiples reglas de correlación que supervisan la actividad inapropiada en la red.	Exigido	SI	
	La solución debe proporcionar en la interfaz del usuario un wizard con la capacidad para minimizar los falsos positivos y entregar resultados precisos del ambiente.	Exigido	SI	

Fernando F. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe brindar la capacidad de correlacionar resultados del análisis de vulnerabilidad de productos de terceros, como por ejemplo Nmap, entre otros.	Exigido	SI	
	La solución debe poseer la capacidad de tomar medidas tras haber recibido una alerta. Por ejemplo, la solución debe poder iniciar scripts o enviar un mensaje de correo electrónico.	Exigido	SI	
Gestión de Logs	La solución debe proporcionar la capacidad de normalizar campos de eventos globales que no están representados por los campos normalizados por defecto.	Exigido	SI	
	La solución debe normalizar campos comunes de eventos (es decir, nombres de usuarios, direcciones IP, nombres de host e inicio sesión dispositivo fuente, etc) de los dispositivos dispares a través de la red de múltiples proveedores.	Exigido	SI	
	La solución debe proporcionar la capacidad de almacenar / conservar registros tanto normalizados como el formato en bruto original del registro de eventos para fines forenses.	Exigido	SI	
	La solución debe almacenar y realizar el archivado de logs en storage externos. Debe proveer mecanismos de compresión de datos. Falta agregar periodo de retención para registros históricos y los de acceso rápido.	Exigido	SI	
	La solución debe proporcionar recopilación sin agentes de los registros de eventos siempre que sea posible.	Exigido	SI	
	La solución debe tener una recopilación de registros y la arquitectura de archivo que admita tanto a corto plazo (en línea) y largo plazo (sin conexión) de almacenamiento de eventos.	Exigido	SI	
	La solución debe proporcionar una taxonomía común de evento.	Exigido	SI	
	La solución debe ser compatible con el acceso a largo plazo a los eventos de seguridad detallada y datos de flujo de red. El sistema debe ser capaz de proporcionar el acceso a al menos x meses el valor de la información detallada.	Exigido	SI	
	La solución debe ser compatible con los métodos de recopilación de logs de la industria (syslog, WMI, JDBC, SNMP, Checkpoint LEA, OPSEC, registros de FTP, SCP, SFTP). Así mismo deberá proveer para MS Windows una herramienta para la exportación de logs de sistema operativo y distintos aplicativos de syslog. Dicha herramienta deberá encolar el envío de datos (por intermitencia de red), limitar la cantidad de EPS y gestionar franjas de horario para evitar saturar el enlace en horario pico.	Exigido	SI	
	La solución debe proporcionar la capacidad de distribuir tanto el almacenamiento y el procesamiento de eventos a través de todo el despliegue de gestión de LOGs/ SIEM.	Exigido	SI	
	La solución debe normalizar las marcas de tiempo de eventos a través de múltiples zonas horarias.	Exigido	SI	

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS Dirección Administrativa DCA

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Flujo SIEM	La solución debe proporcionar un mecanismo para el seguimiento de los incidentes de seguridad a través de una amplia gama de atributos relevantes (es decir, direcciones IP, nombres de usuario, dirección MAC, de registro de origen, reglas de correlación, definido por el usuario, etc.) El usuario debe ser capaz de filtrar los incidentes a lo largo de estos atributos definidos.	Exigido	SI	
	La solución debe poseer un mecanismo para capturar todos los aspectos relevantes de un incidente de seguridad en una sola vista lógica. Esta visión debe incluir hechos relevantes, datos de actividad de la red, alertas correlacionadas, datos de vulnerabilidades, etc.	Exigido	SI	
	La solución debe proporcionar capacidad de enviar notificación de alertas correlacionadas a través de procedimientos bien definidos (es decir, traps SNMP, correo electrónico, etc).	Exigido	SI	
	La solución debe proporcionar una integración con aplicaciones de ticketing systems / mesa de ayuda de la DNCP.	Exigido	SI	
	La solución debe proporcionar un mecanismo para marcar incidente de seguridad/ofensas, y dirigirlas por el personal de las operaciones de seguridad.	Exigido	SI	
Monitoreo de red	La solución debe aprender dinámicamente las normas de comportamiento y exponer los cambios que se producen.	Exigido	SI	
	La solución debe recopilar y el analizar los datos de captura de paquetes.	Exigido	SI	
	La solución debe ser capaz de generar perfiles de la comunicación procedentes de o con destino a la Internet por regiones geográficas en tiempo real.	Exigido	SI	
	La solución debe perfilar el tráfico por el puerto TCP y UDP.	Exigido	SI	
	La solución debe mostrar perfiles de tráfico visuales en términos de bytes, Paquetes y el número de hosts que se comunican. Estas pantallas deben estar disponibles para las aplicaciones, puertos, protocolos, las amenazas y cada punto de control en la red. Todos estos puntos de vista deben apoyar vista específica ubicación de la red de manera que puedan presentar la información de un solo lugar, toda la red o cualquier otro conjunto definido de hosts.	Exigido	SI	
	La solución debe poseer perfiles de tráfico basado en direcciones IP, grupos de direcciones IP, los pares de IP de origen / destino, etc	Exigido	SI	
	La solución debe presentar la información en varios marcos de tiempo. El rango de selección deberá ser como mínimo mes, semanas, día, hora, minutos.	Exigido	SI	
	La solución debe identificar el tráfico de red dentro de un entorno de red virtual.	Exigido	SI	

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe detectar la definición de aplicación más allá de protocolo y puerto. El sistema debe identificar las aplicaciones que utilizan puertos distintos a los conocidos, y la construcción de túneles a sí mismos en otros puertos (por ejemplo, HTTP como transporte para MS-Instant Messenger debe ser detectada como mensajero instantáneo - no HTTP).	Exigido	SI	
	La solución debe proporcionar la capacidad de extraer datos específicos, definidos por el usuario, los campos de los datos de captura de paquetes y el uso de los campos de reglas de correlación.	Exigido	SI	
	La solución debe identificar el tráfico de red de las aplicaciones potencialmente peligrosas (por ejemplo, el intercambio de archivos, peer-to-peer, juegos, etc.	Exigido	SI	
	La solución debe detectar ataques de denegación de servicio (DoS) y distribuidos de denegación de servicio (DDoS).	Exigido	SI	
	La solución debe crear perfiles claramente independientes y diferenciados de tráfico local vs el tráfico con origen o destino a internet.	Exigido	SI	
	La solución debe detectar y presentar vistas actuales de tráficos relativos a las amenazas observadas en la red.	Exigido	SI	
	La solución debe perfilar el tráfico asociado con el diseño lógico de la red (por ejemplo, la subred / CIDR).	Exigido	SI	
	La solución debe permitir al usuario crear perfiles personalizados y vistas usando cualquier propiedad de un flujo, registro, fuente de datos o tráfico que ya está perfilada.	Exigido	SI	
	La solución debe mostrar perfiles de tráfico en términos de tasa de paquetes. Esta capacidad debe estar disponible para el análisis TCP simples (flags TCP, etc.) y la información basada en la frecuencia, (por ejemplo, aplicaciones)	Exigido	SI	
Gestión de Amenazas	La solución debe analizar y correlacionar la información recogida a partir de soluciones de bases de datos como mínimo: PostgreSQL, DB2, MSSQL, MySQL, mariaDB.	Exigido	SI	
	La solución debe cambiar automáticamente las ponderaciones de credibilidad de los dispositivos de seguridad en respuesta a los ataques a nivel de red.	Exigido	SI	
	La solución debe soportar colección de información de los software de Monitoreo de Actividad de base de datos que a su vez estan por soportados por PostgreSQL, DB2, MSSQL, MySQL, mariaDB.	Exigido	SI	
	La solución debe colectar información de las herramientas de administración y gestión de base de datos a al menos Pgbadger, postgreSQL stats.	Exigido	SI	
	La solución debe poseer, la capacidad de contextualizar la actividad de las aplicaciones en la red con los eventos de seguridad de los dispositivos monitoreados.	Exigido	SI	

Fernando I. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Iniante
Asesor Técnico - Legal
DNCP

	La solución debe proporcionar una vista de eventos en tiempo real de la información monitorizada en crudo/original, a corto plazo y a largo plazo.	Exigido	SI	
	La solución debe proporcionar una vista de eventos en tiempo real, tanto en crudo (original) como en una vista normalizada.	Exigido	SI	
	La solución debe proporcionar una vista de eventos que ocurrieron en un corto plazo atrás, tanto en crudo como en una vista normalizada. El acceso deberá ser rápido para reportes, consultas e investigación de los eventos. Es considerado 7 días de retención para el periodo de corto plazo. Este periodo de retención debe ser modificable y ajustable a lo largo del tiempo conforme necesidades de la DNCP.	Exigido	SI	
	La solución debe proporcionar una vista de eventos que ocurrieron en un largo plazo atrás, tanto en crudo como en una vista normalizada. El acceso será para reportes, consultas e investigación de los eventos bajo demanda o programadas. Es considerado 30 días de retención para el periodo de largo plazo. Este periodo de retención debe ser modificable y ajustable a lo largo del tiempo conforme necesidades de la DNCP.	Exigido	SI	
	La solución debe poseer, la capacidad de contextualizar los eventos de seguridad de reportados con el knowledge en tiempo real de los activos que están siendo monitoreados.	Exigido	SI	
	La solución debe analizar y correlacionar, la información recogida de los sistemas de backup utilizado tanto para servidores como para estaciones de trabajo.	Exigido	SI	
	La solución debe poseer la capacidad de priorizar por peso determinado, en forma automática la prioridad de los sucesos de seguridad notificados de acuerdo con la importancia relativa del dispositivo monitoreado.	Exigido	SI	
	La solución debe poseer la capacidad de priorizar por preso en forma automática la gravedad de los sucesos de seguridad notificados de acuerdo a la vulnerabilidad de los dispositivos monitoreados.	Exigido	SI	
	La solución debe analizar y correlacionar, la información recogida de sistemas propietarios de la DNCP.	Exigido	SI	
	La solución debe posser la capacidad de asignar calificaciones de credibilidad a los dispositivos de seguridad monitoreados.	Exigido	SI	
	La solución debe cambiar automáticamente las ponderaciones de credibilidad de los dispositivos de seguridad en respuesta a los ataques a nivel de red	Exigido	SI	
	La solución deberá soportar colectar información de software de seguridad específicos para monitoreo de actividad e integridad de archivos.	Exigido	SI	
	La solución debe procesar información recolectada de los Network Flow (NetFlow, sflow) utilizados por la DNCP.	Exigido	SI	
	La solución debe procesar información colectada de los sistemas de gestión de redes.	Exigido	SI	

Fernando R. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe procesar información colectada de los scanner de vulnerabilidad, como mínimo Nmap.	Exigido	SI	
	La solución debe procesar información colectada de los productos de Directorios utilizados por la DNCP, como mínimo Active Directory, LDAP.	Exigido	SI	
	La solución debe figurar dentro del cuadrante Magico de Gartner en el último informe.	Exigido	SI	
Origen de Datos	La solución debe ser compatible como mínimo con los siguientes productos de fabricantes, en el caso de no serlo deberá desarrollar los conectores necesarios para una óptima colección de la información.	Exigido	SI	
	Apache HTTP Server			
	UPS Emerson			
	UPS Powerware			
	Cisco ACE			
	Cisco Aironet			
	Cisco Call Manager			
	Cisco UCCX			
	Cisco Nexus			
	Cisco IOS			
	Cisco Wireless LAN Controllers			
	Cisco ASA			
	Jboss application server			
	Tomcat aplication Server			
	Netty aplication server			
	PostgreSQL			
	mariaDB			
	MySQL			
	IBM DB2			
	IBM WebSphere Application Server			
	IBM INTM			
	IBM TSM			
	IBM ITSM			
	IBM TEPS			
	IBM TEMS			
	Microsoft Exchange Server			
	Microsoft Forefront Threat Management Gateway			
	Microsoft Forefront Endpoint Protection			
	Microsoft SQL			
	Microsoft SharePoint			
	Microsoft Windows Security Event Log			
	Microsoft windows servidor genérico			
	Microsoft windows 7			
	Microsoft Active Directory			
	Microsoft lync server			

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS - Dirección Administrativa - UOC

Fernando F. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	Microsoft file server			
	Microsoft dns server			
	Microsoft sccm server			
	Linux servidor genérico – OS			
	Linux Generic – Iptables			
	Linux Squid proxy			
	Red Hat Enterprise Virtualization			
	Vmware Virtualization			
	Play Web Framework for Java			
	Gray Log server			
	PgBagder log analyzer for PostgreSQL.			
	Postgrestats - Statistics for de postgresql database			
	La solución debe analizar y correlacionar información recogida de los servidores basados en Linux / UNIX, Microsoft Windows, estaciones de trabajo Windows y Linux, y sistemas de usuario final.	Exigido	SI	
	La solución debe importar custom logs desde múltiples aplicaciones y formatos diversos de logs, tales como XML, CSV, incluso complejos, como multilinea (donde un mismo evento está compuesto por varias líneas del log).	Exigido	SI	
	La solución debe soportar recolectar/analizar la información de las herramientas de FIM/FAM.	Deseable	-	-
	La solución debe soportar recolectar/analizar la información de escaneres de vulnerabilidad.	Exigido	SI	
	La solución debe recolectar/analizar la información de Netflow/Sflow	Exigido	SI	
	La solución debe recolectar/analizar la información de aplicaciones propietarias de la DNCP.	Exigido	SI	
	La solución debe recolectar/analizar la información de la infraestructura de red, como minimo Cisco Switches, Router, firewall, IDS, IPS	Exigido	SI	
	La solución debe recolectar/analizar la información de los servicios de directorio como mínimo de: Microsoft Active Directory, LDAP.	Exigido	SI	
Reportes	La solución debe proporcionar reportes, sobre todos los elementos disponibles para la gestión a través de la interfaz gráfica de usuario.	Exigido	SI	
	La solución debe proporcionar un motor de informes configurable para la creación de informes personalizados.	Exigido	SI	
	La solución debe realizar reportes schedulados, a ser por hora, día, semanal, mensual.	Exigido	SI	
	La solución debe poseer plantillas para la creación y entrega de informes en múltiples niveles que van desde operaciones a actividades específicas de la DNCP.	Exigido	SI	
	La solución debe proporcionar informes out-of-the-box', para las cuestiones operativas típicas del negocio, como mínimo reportes de :	Exigido	SI	
	Autenticación			

Fernando I. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	Identidad			
	Actividad del usuario			
	Compliance			
	Gestión de configuraciones y cambios			
	Gestión de red			
	Seguridad			
	Monitoreo de uso			
	Actividad de las aplicaciones			
	Informes específicos por dispositivos, todos los activos (sistema operativos, base de datos, etc.)			
	Gerenciales / Ejecutivos			
	La solución debe proporcionar reportes out-of-the-box de cumplimiento de las regulaciones específicas (PCI, SOX, FISMA) y marcos de control incluidos (NIST, COBIT, ISO).	Exigido	SI	
	La solución debe proporcionar un "Dashboard" para la visualización rápida de reportes de seguridad y la información de red. Como mínimo debe brindar:	Exigido	SI	
	Cualquier búsqueda de eventos o flow.			
	Lista y estados de incidentes y ataques (ofensas).			
	Top de ofensas, por destino, categoría y origen.			
	Top de eventos por severidad.			
	Top de eventos por origen.			
	Estado del sistema			
	Reportes generados recientemente			
	La solución debe realizar la generación automática de informes, en los siguientes formatos como mínimo:	Exigido	SI	
	HTML			
	PDF			
	XML			
	CSV/XLS			
	RTF			
	La solución debe realizar informes de tendencias históricas.	Exigido	SI	
	La solución debe realizar y entregar reportes de vulnerabilidades en forma centralizada.	Exigido	SI	
	La solución debe realizar y entregar informes de activos.	Exigido	SI	
Arquitectura	La solución debe integrarse con otras soluciones de seguridad y de inteligencia de red.	Exigido	SI	
	La solución debe permitir la personalización, para satisfacer las necesidades únicas de la entidad.	Exigido	SI	
	La solución debe poder ampliarse/expandirse fácilmente para apoyar la demanda adicional.	Exigido	SI	
	La solución debe poseer una base de datos distribuida para los eventos y actividad de la red de tal manera que toda la información se puede acceder desde una única interfaz de usuario.	Exigido	SI	

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

	La solución debe garantizar la integridad de la información recogida a través de hashing SHA-1, SHA2. Además debe contar con mecanismos de control y comprobación de integridad, que debe informar y advertir la manipulación de archivos.	Exigido	SI	
	La solución debe proporcionar mecanismos intuitivos para la solución de problemas, tales como notificaciones proactivas, las utilidades de línea de comandos.	Exigido	SI	
	La solución debe poseer un modelo distribuido para la correlación de tal manera que los contadores, las secuencias, las búsquedas de identidad, etc sean compartidos por todos los colectores. Es decir, buscar 10 fallos de conexión del mismo nombre de usuario seguido de un único inicio de sesión correcto para ese mismo nombre de usuario, donde los eventos vistos por un solo colector no superan el umbral de 10, pero a través de múltiples colectores superaría el umbral.	Exigido	SI	
	La solución debe ser compatible con la taxonomía de la entidad en cuanto a eventos y campos. El usuario debe ser capaz de añadir sus propios nombres de eventos únicos (es decir, la posibilidad de añadir nuevos campos que no forman parte del esquema default).	Exigido	SI	
	La solución debe permitir el tag personalizada de eventos, debe proporcionar la recuperación transparente, la agregación, clasificación, filtrado y análisis de datos a través de todos los componentes distribuidos.	Exigido	SI	
	La solución deberá estar diseñado para almacenar la información referida a todos los productos de fabricantes citados anteriormente, además de los otros requerimientos citados en los diferentes puntos de las especificaciones técnicas, clasificados en información en tiempo real, información referida a un periodo corto de tiempo correspondiente a 7 días, e información referida a un periodo largo de tiempo correspondiente a 30 días.	Exigido	SI	
	La solución debe poseer una arquitectura escalable y distribuida, contar con base de datos federadas, con el fin de correlacionar y almacenar grandes volúmenes de datos en tiempo real, que puedan agregarse nodos de monitoreo/correlación a la solución para incrementar su capacidad de procesamiento de eventos y correlación.	Exigido	SI	
	Debe poder escalar hasta al menos 2.000 EPS en la misma appliance o solución virtual ofertada.	Exigido	SI	
	La solución debe incluir, instalación, configuración y puesta punto sin afectar el ambiente de producción de la DNCP. Además el oferente deberá incluir en su oferta todo lo necesario para el correcto funcionamiento, licencias, hardware, cables, accesorios, tanto para la forma appliance o solución virtual. El fabricante deberá avalar que la capacidad del harware ofertado cumple con los requerimientos exigidos.	Exigido	SI	El hardware ofertado está basado en las recomendaciones del fabricante. Adjunto Manuel del fabricante página 17-18 del manual IBM Installation Guide.

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Fernando M. Caballero Zunis
Coordinador de Seguridad de la Información
DTI - DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Garantía	Garantía escrita de 1 año emitida por el fabricante o su representante oficial en Paraguay por la solución ofertada. Debe incluir 12 meses de soporte local que deberá ser ejecutado por los técnicos locales certificados del oferente, incluirá acceso a actualizaciones, a la base de datos de conocimientos, y escalamiento a centros de soporte superiores del fabricante, para la resolución de problemas relacionados a la solución.	Exigido	SI	
Plan de Trabajo	Deberá presentar un plan de trabajo que contemple todas las actividades del proyecto, con sus respectivos plazos de tiempo aproximados y los recursos asignados al mismo, considerando el plazo del plan de entrega del presente pliego.	Exigido	SI	
Capacitación	Elaborar y ejecutar un plan de adiestramiento para 3 funcionarios de la DNCP. El mismo debe contemplar entrenamiento en todas las funcionalidades con la que cuenta la solución a ser implementada, y deberá tener una duración total de 40 horas.	Exigido	SI	
Carta del Fabricante	El proveedor deberá presentar una carta del fabricante o su representante oficial en Paraguay, en la cual avale que el mismo se encuentra en condiciones y autorizado para la venta, instalación, configuración y soporte de la solución ofertada.	Exigido	SI	

Sección VII - Anexos - Anexo I - Documentos que componen la oferta	
G) Documentos adicionales a la oferta que demuestren que los Bienes o Servicios ofertados cumplen con las especificaciones de la Sección III, Suministros Requeridos	
Certificación de los técnicos locales propuestos.	Cumple
Un listado de las licencias y hardware que se proveerán para cumplir con la solución requerida.	Cumple

De acuerdo a lo establecido en el Articulo 59 *"Disconformidades, errores y omisiones"* del Decreto 21909/03, se ha solicitado, mediante nota en fecha 14/10/2015, la presentación de documentaciones necesarias para corroborar el cumplimento de las especificaciones técnicas. Se ha recibido en tiempo y forma dicha documentación, cumpliendo así con lo solicitado para la parte técnica.

A continuación se pasa a verificar la documentación, de acuerdo a lo solicitado en el PBC. La misma se detalla en la siguiente planilla:

Documentos	**STARK TECNOLOGIA S.A.**
	Cumple/No Cumple
Formulario de Oferta	Cumple
Garantía de Mantenimiento de Oferta	Cumple

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Bicagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Fotocopia autenticada de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos.	Cumple (SIPE)
Fotocopia autenticada de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); ó los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas.	Cumple (SIPE)
Declaración jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03, de acuerdo con lo dispuesto en la Resolución N° 330/07 de la Dirección General de Contrataciones Públicas.	Cumple (SIPE)

A continuación se verifica la documentación formal presentada. La misma se detalla en la siguiente planilla:

Documentos formales	STARK TECNOLOGIA S.A.
Declaración Jurada en la que se garantice que el oferente no se encuentra involucrado en prácticas que violen derechos de los menores estipulados en la Constitución Nacional, los Convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el Código del Trabajo, Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la República del Paraguay, conforme al formato aprobado por la Dirección Nacional de Contrataciones Públicas en la Resolución DNCP Nº 941/2010.	Cumple (SIPE)
Fotocopia simple de la cédula tributaria (constancia de inscripción en el Registro Único de Contribuyentes RUC) y de los Documentos de Identidad de los representantes o apoderados de la Sociedad.	Cumple
Fotocopia autenticada de la declaración de IVA del último mes vencido y/o del Impuesto a la Renta o Certificado de Cumplimiento Tributario expedido en el mes anterior a la presentación de la oferta.	Cumple
Autorización del Fabricante, Representante o Distribuidor en caso de que la empresa oferente no haya fabricado o elaborado el producto ofertado, sino sea importador y/o distribuidor de los bienes.	Cumple
Planilla de Especificaciones Técnicas.	Cumple
Certificación de los técnicos locales propuestos.	Cumple
Folletos técnicos de la funcionalidad de la solución ofertada.	Cumple
Un listado de las licencias y hardware que se proveerán para cumplir con la solución requerida	Cumple
Balances de los años 2012, 2013, 2014.	Cumple
Ratios financieros	Cumple
Copia de contratos y/o facturaciones de ventas con sus respectivas constancias de implementación que avalen la experiencia local en la implementación de la solución tipo SIEM (años 2013, 2014, 2015).	Cumple
Certificaciones de los técnicos propuestos.	Cumple
Un listado de las licencias y hardware que se proveerán para cumplir con la solución requerida. El listado del hardware debe incluir marca, modelo y cantidad.	Cumple
Certificado de Origen Nacional	No presenta

Seguidamente, conforme a los criterios de calificación establecidos en el PBC, se ha procedido a verificar si el Oferente no se encuentra comprendido en las prohibiciones establecidas en el Art. 40, incisos a) y b) de la Ley 2051/03, en base al siguiente análisis:

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Documento	STARK TECNOLOGIA S.A. Cumple/No Cumple
Presentación satisfactoria de la Declaración Jurada de no hallarse comprendido en las prohibiciones y limitaciones establecidas en el Artículo 40 de la Ley N° 2051/03.	Cumple
Inciso a): Verificación de los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso "a" del Artículo 40.	Sin registros
Inciso b): Verificación por los medios disponibles, si el Oferente y los demás sujetos individualizados en las prohibiciones contenidas en la Ley N° 1626/00 "De la Función Pública", aparecen en la base de datos del SINARH o bien de la Secretaría de la Función Pública.	Sin registros (SINARH)

Datos corroborados de la base de datos del SINARH.

Seguidamente, la convocante analiza los requisitos de calificación posterior del Oferente, de conformidad con lo establecido en la Cláusula 36 de las IAO, empleando los requisitos estipulados.

STARK TECNOLOGIA S.A.						
	RATIO DE LIQUIDEZ					
		2.014	2.013	2.012	Suma	Promedio
	Activo Corriente	8.961.160.756	5.473.127.628	2.090.276.548	5,65	1,88
	Pasivo Corriente	6.758.486.073	3.272.950.731	788.494.957		
	Ratio de Liquidez	1,33	1,67	2,65		
	ENDEUDAMIENTO					
		2.014	2.013	2.012	Suma	Promedio
	Pasivo Total	6.758.486.073	3.272.950.731	788.494.957	1,59	0,53
	Activo Total	10.078.625.249	5.696.067.850	2.297.357.429		
	Ratio de Endeudamiento	0,67	0,57	0,34		
	RENTABILIDAD					
		2.014	2.013	2.012	Suma	Promedio
	Utilidad después de impuestos	1.053.181.050	861.161.745	484.208.634	799,52	266,51
	Capital	300.000.000	300.000.000	300.000.000		
	Ratio de Rentabilidad	351,06	287,05	161,40		%

Requisitos De Calificación	Criterio
a) Capacidad financiera	
a. Ratio de Liquidez: activo corriente / pasivo corriente: Deberá ser igual o mayor que 1, en promedio, en los 3 últimos años	Cumple
b. Endeudamiento: pasivo total / activo total: No deberá ser mayor a 0.80 en promedio, en los 3 últimos años	Cumple
c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los últimos 3 años no deberá ser negativo	Cumple
b) Experiencia y Capacidad Técnica	
El oferente o el representante oficial de la herramienta ofertada deberá contar con al menos 1 (una) experiencia dentro del territorio nacional en la implementación de la solución tipo SIEM con una capacidad mínima de EPS y FPM a lo requerido en el presente llamado. Para avalar este requerimiento podrá presentar copia de contratos y/o facturaciones de ventas y sus respectivas constancias de satisfacción del cliente, y deberá contar con los datos del contacto, alcance del proyecto y personal responsable de la ejecución. Estas implementaciones podrán ser de instituciones públicas y/o privadas. (Años 2013, 2014 y 2015).	Cumple
El oferente deberá contar con al menos 2 técnicos locales certificados en la solución tipo SIEM de la marca ofertada o fabricante.	Cumple

Fernando Y. Caballero Yunis
Coordinador de Seguridad de la Información
DTI - DNCP

Lic. Noelia Ricagno
Dirección Administrativa
DNCP

Abg. Juan Humberto Báez Infante
Asesor Técnico - Legal
DNCP

Mediante el análisis, se pudo determinar que la firma **STARK TECNOLOGIA S.A.** cumple con las condiciones legales, técnicas y económicas establecidas en el Pliego de Bases y Condiciones, por lo que se recomienda su adjudicación.

6. Motivos de calificación

Atendiendo a lo dispuesto en el Artículo 28° de la Ley 2051/03 "De Contrataciones Públicas" y de conformidad al Artículo 63 del Decreto Reglamentario Nº 21909/03, *"...la adjudicación deberá recaer en el oferente cuya oferta: 1) cumpla con las condiciones legales y técnicas estipuladas en el PBC; 2) tenga las calificaciones y la capacidad necesaria para ejecutar el contrato; 3) Presente el precio evaluado como el más bajo"*, la firma **STARK TECNOLOGIA S.A.**, cumple satisfactoriamente los requisitos solicitados.

7. Conclusión o recomendación de adjudicación

En base a las consideraciones expuestas en el presente informe, y de conformidad a los Artículos 27 y 28 de la Ley Nº 2051/03 y los Artículos 58 al 63 del Decreto Reglamentario Nº 21909/03, el Comité de Evaluación recomienda ADJUDICAR, por ser una oferta conveniente a los intereses institucionales, por cumplir con las especificaciones técnicas requeridas, las condiciones legales y la capacidad necesaria para responder a los compromisos asumidos; a la firma **STARK TECNOLOGIA S.A.**, por un monto total de Gs. 395.000.000 (guaraníes trescientos noventa y cinco millones).

Es nuestro informe.

Sr. Fernando Caballero | Lic. Noelia Ricagno | Abg. Humberto Báez

Asunción, 14 de octubre de 2015

Señores
STARK TECNOLOGIA S.A.
Presente

Me dirijo a usted, con referencia a su oferta presentada para el llamado a Licitación por Concurso de Ofertas N° 15/2015 "**ADQUISICION DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y GESTION DE EVENTOS (SIEM)",** y teniendo en cuenta las facultades previstas en el Artículo 59 "Disconformidades, errores y omisiones" del Decreto 21909/03, requerimos los siguientes documentos solicitados en el PBC:

a. Para el ítem 1 – Adquisición de un sistema de información de seguridad y gestión de eventos, en la sección "Capacitación" se requiere lo siguiente:

Capacitación	Elaborar y ejecutar un plan de adiestramiento para 3 funcionarios de la DNCP. El mismo debe contemplar entrenamiento en todas las funcionalidades con la que cuenta la solución a ser implementada, y deberá tener una duración total de 40 horas.	Exigido

Favor remitir dicho plan.

b. Para el ítem 1, sección VII. "Anexos", Documentos que componen la oferta, el punto G) dicta lo siguiente:

G) Documentos adicionales a la oferta que demuestren que los Bienes o Servicios ofertados cumplen con las especificaciones de la Sección III, Suministros Requeridos.
Un listado de las licencias y hardware que se proveerán para cumplir con la solución requerida.

Favor remitir el mencionado listado.

La documentación requerida deberá ser presentada a esta Dirección Nacional vía email a uoc4@dncp.gov.py, a más tardar hasta el día de mañana jueves 15 del corriente hasta las 11:00 hs., a fin de proseguir con el proceso de evaluación correspondiente.

Atentamente,

DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS
Dirección Administrativa

C.P. Nathalia Melot
Coordinadora de Adquisiciones

Alba Noelia Ricagno Espinoza

De: Alba Noelia Ricagno Espinoza
Enviado el: miércoles, 14 de octubre de 2015 09:11 a.m.
Para: 'mnunez@stark.com.py'
Asunto: llamado a Licitación por Concurso de Ofertas N° 15/2015 "ADQUISICION DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y GESTION DE EVENTOS (SIEM)",
Datos adjuntos: CONSULTA STARK 14-10-150000.pdf

En adjunto envío nota.

Favor confirmar recepción del presente.

Atte,

LIC. NOELIA RICAGNO
UOC

Alba Noelia Ricagno Espinoza

De: Mirian Cardozo <contabilidad@stark.com.py>
Enviado el: jueves, 15 de octubre de 2015 08:49 a.m.
Para: Alba Noelia Ricagno Espinoza
CC: Martin Nuñez
Asunto: Re: llamado a Licitación por Concurso de Ofertas N° 15/2015 "ADQUISICION DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y GESTION DE EVENTOS (SIEM)",
Datos adjuntos: Plan Cap SIEM.pdf; Lista Componentes SIEM.pdf

Buenos dias Adjunto los Documentos solicitados.

Favor confirmar recepcion de mail.
Saludos

El 15 de octubre de 2015, 8:41, Martin Nuñez <mnunez@stark.com.py> escribió:

---------- Mensaje reenviado ----------
De: **Alba Noelia Ricagno Espinoza** <uoc4@dncp.gov.py>
Fecha: 14 de octubre de 2015, 9:10
Asunto: llamado a Licitación por Concurso de Ofertas N° 15/2015 "ADQUISICION DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y GESTION DE EVENTOS (SIEM)",
Para: "mnunez@stark.com.py" <mnunez@stark.com.py>

En adjunto envío nota.

Favor confirmar recepción del presente.

Atte,

LIC. NOELIA RICAGNO

UOC

Antes de imprimir este mensaje, piense si es necesario hacerlo. Al reducir el uso de papel se evita la generación de residuos, el consumo de los recursos naturales (madera, agua, energía) y los problemas de contaminación que ocasiona la producción de papel.

--

Mirian Cadozo Careaga

PLAN DE CAPACITACION IBM SECURITY QRADAR

ETAPA	ALCANCE DE ACTIVIDADES	DURACION HORAS
Capacitación Qradar	DIA 1 • Introducción • Seguridad de Red • Dashboard	8
	DIA 2 • Log Activity • Network Activity • Filtro Avanzado • Activos y vulnerabilidades	8
	DIA 3 • Ofensas • Investigacion de Ofensas • Reglas	8
	DIA 4 • Tuning • Reporting • Soporte	8
	DIA 5 • Custom Log • Creacion de reglas	8

Prerequisitos

- Los participantes deberán contar con una notebook/Destop con 8 GB de memoria RAM y vmware player o esxi instalado para la instalación de los virtual apliance
- El taller ser llevar a cabo sobre servidores virtuales configurados específicamente para el mismo
- Sera realizada en las instalaciones de la DNCP

STARK TECNOLOGÍA S.A

LISTADO COMPONENTES

IBM SECURITY QRADAR SIEM

Cantidad	Numero de Parte	Descripción
1	D0WSCLL	IBM Security Qradar SIEM All-in-One Virtual 3190 Install License + SW Subscription 12 Months
4	D0WUKLL	IBM Security Qradar Virtual SIEM Event Capacity Increase of 100 EPS Install License + SW Subscription 12 Months
1	D10UVLL	IBM Security Qradar SIEM Event Capactity Increase to 1K EPS from 500 EPS Install License + SW Subscription & Support 12 Months
1	VS6-ESSL-KIT-C	VMware vSphere 6 Essentials Kit for 3 hosts (Max 2 processors per host)
1	5462-C2U	X3650 M5, Xeon 6C E5 2.4 GHz., 96 GB de ram TRUDDR4, 4 HDD 600 Gb SAS 2.5, Server RAID M5200, Dual 550W Power Supply, UltraSlim SATA DVD-ROM

STARK
TECNOLOGÍA S.A.