FIDUPREVISORA S.A.
INVITACIÓN A COTIZAR No. 027 de 2022
RESPUESTA A OBSERVACIONES

FIDUPREVISORA S.A. se permite dar respuesta a cada una de las observaciones presentadas, en relación con la invitación a cotizar No. 027 de 2022 que tiene por objeto "Fiduprevisora S.A. a través de la Gerencia de Riesgos está interesada en recibir cotizaciones para contratar una solución para prestar el servicio de SOC (Security Operation Center) con correlacionador de eventos de seguridad, realizar análisis de vulnerabilidades y pruebas de Ethical Hacking con personal experto, en horario 7*24, esto con el fin de monitorear y dar respuesta a los incidentes de seguridad de la infraestructura tecnológica en cumplimiento a los dispuesto en la circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia y la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia".

OBSERVANTE No. 1

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
7	17/06/2022 2:45 PM	lizbeth.kure@digiware.net	**DIGIWARE**

1. Número de servidores de aplicaciones, Bases de Datos, correo, DNS, que presten servicios a los usuarios.

RESPUESTA FIDUPREVISORA S.A: 145 servidores de aplicaciones, 30 Bases de Datos, DNS.

2. ¿Posee la entidad fuentes de Cloud? Azure, Amazon, O365, otros servicios de Ciberseguridad EDR, Endpoints, etc que se consuman en cloud.

RESPUESTA FIDUPREVISORA S.A: Sí.

3. Solicitamos nos aclaren para la retención de la información y para análisis o tiempo que se requiere para guardar logs y que modalidad: Hot – Datos 100% disponibles para búsquedas rápidas, Dashboards y reportes (1 mes recomendado)
   Warm – Datos 100% disponibles para búsquedas y reportes (3 a 6 meses recomendado)
   Frozen – Datos congelados, no disponibles para búsquedas y reportes. Pero requeridos por auditoría.

RESPUESTA FIDUPREVISORA S.A: Sugerimos 12 meses

4. ¿Cuáles son las fuentes de las herramientas que generan bitácoras de acceso o actividad? ¿Marca? Firewall, VPN, Proxy, Endpoint, Servidores Unix, Windows, Active Directory, SandBox, Mail Security, CASB, Azure, Amazon, GCP, Cloud Productivity SaaS, Office 365, GSuite.

RESPUESTA FIDUPREVISORA S.A: La pregunta: firewall (marca: 1 Fortigate 1200D con alta disponibilidad), servidor AD (Microsoft server 2012).

5. ¿Qué servidor de correo manejan?

RESPUESTA FIDUPREVISORA S.A: RTA: Microsoft office 365

6. ¿Qué NAC tienen?

RESPUESTA FIDUPREVISORA S.A: Clearpass de cisco

7. ¿Qué Directorio Activo tienen?

RESPUESTA FIDUPREVISORA S.A: Servidor AD (Microsoft server 2012).

OBSERVANTE No. 2

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
22	17/06/2022 4:12 PM	SECOP II	**TELEFONICA**

2.2. ESPECIFICACIONES TECNICAS DEL SERVICIO

1. Numeral 1: A que se refieren con alta disponibilidad, se refieren a tener dos SOC operados desde distintas locaciones o la alta disponibilidad de los componentes de hardware o sistemas que componen el servicio. RTA: Alta disponibilidad hace referencia disposición tecnológica, técnica y humana que aseguren la verificación, control y seguimiento de la calidad y niveles de servicio, con miras a permitir el monitoreo continuo.
2. Numeral 3: ¿De los 400 activos que hacen referencia, estiman un crecimiento esperado en el tiempo de servicio? RTA: “capacidad mínima” de cuatrocientos (400) dispositivos.
3. Numeral 9: Agradecemos a la entidad precisar si los 500 eventos por segundo que informan corresponden a la totalidad de los activos a monitorear. Es decir 400, Para efectos de la oferta los rangos representan riesgos en el dimensionamiento del servicio. RTA: Los 500 eventos por segundo EPS (Eventos por Segundo) correlacionando son referentes a los eventos de seguridad de la Infraestructura TI;
4. Numeral 9: ¿Por favor agradezco su ayuda cual es el tiempo de retención de los logs de seguridad filtrados, tanto para los que se deben consultar en línea como los que se guardan en otros medios? RTA: Los log se resguardan 12 meses, en lìnea se pueden consultar siempre ONLINE en el momento que se requieran
5. Numeral 17: ¿En el período cuántos nuevos casos de uso en la detección de incidentes de seguridad y ciberseguridad de la información estima la entidad? RTA: Indefinidos.
6. Numeral 24: USO INDEBIDO DE MARCA
    a. ¿Cuántas marcas a proteger? RTA: No se define una cantidad como tal, teniendo en cuenta que se indica la detección de acciones que atenten contra el buen nombre de la

entidad y estas pueden identificarse de muchas maneras (en la invitación se indican 4 ellas)

b. ¿Cuál es la cantidad de take down? RTA: no hay límite, los que sean necesarios.

7. Numeral 24: OTRAS: *Activar mecanismos de intercambio de información de amenazas con diferentes fuentes de la misma, ya sean públicas o privadas, para mejorar la proactividad en la detección y la protección.*
   Cuántas fuentes de información espera tener alcance la entidad en especial las privadas, entendiendo que las públicas no tienen costo y las privadas son por pago. RTA: No se define un numero teniendo en cuenta que entre los mecanismos de intercambio esta OneDrive, SharePoint entre otros.
8. Numeral 24: OTRAS: *Contar con espacios de discusión sobre nuevas técnicas de ataques, herramientas de seguridad, mejores prácticas, etc.*
   a. ¿Cuántas charlas al año? Para cuántas personas RTA: Se solicita disponibilidad de consultas y discusiones "técnicas" permanente 87*24) y las sesiones serian a demanda.
9. Numeral 26: Por favor especificar la cantidad de FW y las marcas de la infraestructura RTA: 1 Fortigate 1200D con alta disponibilidad
10. Numeral 29: Entendemos que estas funcionalidades requeridas son ajenas a un siem, ésta obedece a funcionalidades de un modelador de ancho de banda, ¿la entidad requiere que se incluya como un servicio aparte? RTA: No
1. Numeral 44: La entidad espera que el servicio tenga un sistema de ticketing aparte o que se integre con el que tiene la entidad. (Aranda) RTA: Se requiere que el proponente tenga una herramienta de tickets pero se pregunta si es posible integrase con Aranda.
11. Numeral 44: La entidad dispone de una herramienta para la gestión integral del riesgo o espera que se incluya este componente, en nuestra experiencia este tipo de integraciones irían adicionales o se gestiona de manera manual con la herramienta integral de la entidad. RTA: Si contamos con una herramienta para la gestión de riesgos.
12. Numeral 56: Cuántas pruebas de red team contemplan al año? RTA: uno por semestre
13. Numeral 57: Solicitamos a la entidad estimar la opción en nube. RTA: si cumple con los requerimientos de un appliance físico no se vería ningún inconveniente.
14. Numeral 58 y 59: de las pruebas de vulnerabilidades que hacen mención por favor informar, cantidad de activos y direcciones Ip's a proteger. RTA: 350.
15. Numeral 60: Entendemos que esto hace referencia a que el soc va generar la gestión cuándo hay una vulnerabilidad y se debe hacer el parcheo por parte del área encargada dueño del activo. Solo se informa si aún existe la vulnerabilidad encontrada. RTA: si (pero si hay acompañamiento y asesoría no sobra el apoyo).
16. Numeral 64: *Realizar dos pruebas de Ethical Hacking externas (caja negra)*
    a. ¿A Cuántos activos? RTA: 15
    b. ¿Entendemos que se harán dos pruebas al año con su retest? RTA: Es correcto
17. Numeral 66: *Realizar análisis estático y dinámico*
    a. ¿Cuántas aplicaciones productivas? RTA: 15
    b. ¿Cuántas aplicaciones en desarrollo? RTA: 10.
    c. ¿Cuántos usuarios en desarrollo se estiman? RTA: 10.
18. Numeral 67: Pruebas de ingeniería social:
    a. ¿Cuántas al año? RTA: 1 por semestre
    b. ¿Presenciales o remotas? RTA: Virtuales

2.2. CONDICIONES DEL SERVICIO REQUERIDO

19. Numeral 7: con respecto a la capacitación solicitada, entendemos que estás son sin certificado, ¿es correcto? RTA: El requerimiento es claro "Este entrenamiento debe ser certificable por parte del proveedor. Máximo para 5 funcionarios.".
20. Numeral 8: cuando se refieren a La solución debe ser reconocida dentro del cuadrante mágico de Gartner u otro analista independiente. ¿Se refieren al siem? RTA: Si
21. Numeral 28: Equipos a monitorear
    a. ¿Cuántos FW Fortinet? RTA: 1 Fortigate 1200D con alta disponibilidad.
    b. Suite Trend Micro (antivirus, antimalware, DLP, device control) (monitoreo SOC)…

    ¿Con este activo se puede gestionar el servicio? RTA: No es clara la pregunta

    c. Suite Trend Micro (antivirus, antimalware, DLP, device control) (monitoreo SOC)…

    ¿Es de la entidad? RTA: Si

    d. Suite Trend Micro (antivirus, antimalware, DLP, device control) (monitoreo SOC)…

    ¿Cuántos agentes lo componen? O solo la consola. RTA: 250

    e. Marca del NAC? RTA: Clearpass de cisco.

    f. Cuando se refieren a página web son 10 aplicaciones web y 10 portales web, Por favor aclarar cantidades. RTA: estas cantidades son correctas.

OBSERVANTE No. 3

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
3	17/06/2022 4:32 PM	zrincon@newnetsa.com	**NEWNET S.A.**

1. En el punto #64. Realizar dos pruebas de Ethical Hacking externas (caja negra). Por favor indicad la cantidad de equipos o IPs a los que hay que desarrollar la pruebas de Ethical hacking. RTA: 15.
2. En el punto #66. Realizar análisis estático y dinámico. Por favor ampliar este alcance. ¿Se requiere análisis de código del desarrollo de aplicaciones?, Si es así, que lenguajes de desarrollo se involucran y cuantas líneas de código por cada aplicación se requieren analizar. RTA: el requerimiento No.66 es callarlo en indicar el requerimiento de los análisis estáticos de código de otra parte se deben tener en cuenta los requisitos del numeral 2.2 ESPECIFICACIONES TECNICAS DEL SERVICIO en particular con lo relacionado con el item 24. Dentro del servicio provisto por el SOC se deberán detectar acciones tales como: EXPLOTACION DE VULNERABILIDADES.
3. En el punto #67. Prueba de Ingeniería social. Por favor indicar ¿cuántas pruebas requieren por año a los 20 funcionarios? RTA: 1 por semestre.

OBSERVANTE No. 4

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
15	17/06/2022 4:38 PM	yohanna.ramirez@wexler.com.co	**WEXLER**

1. Se solicita amablemente a la entidad aclarar si nuestro correcto entendimiento es correcto y se refieren a que el SOC debe contar con mecanismos para garantizar la prestación del servicio de forma ininterrumpida, cumpliendo con los ANS solicitados. RTA: Es correcto.
2. Se solicita muy amablemente a la entidad aclarar si se refieren a que el SIEM debe poderse integrar a las plataformas mencionadas. RTA: A eso nos referimos efectivamente.
3. Se solicita muy amablemente a la entidad indicar los tipos de equipos con los que cuenta para validar el diseño de la solución y la capacidad de integración con los diferentes dispositivos. RTA: No es claro la pregunta.
4. Se solicita muy amablemente a la entidad indicar dispositivos, sedes de más arquitectura. Para poder hacer un correcto diseño de la solución. RTA: Bogotá 919 y en 11 ciudades (96).
5. Se solicita muy amablemente a la entidad quitar la palabra Nativa, ya que las soluciones de SIEM del mercado se pueden integrar con múltiples vender de seguridad para detectar el comportamiento de la solución, pero para validar que la solución se puede integrar de forma nativa es necesario la marca y modelo de los diferentes dispositivos para hacer dicha validación. RTA: No es claro la pregunta.
6. Se solicita muy amablemente a la entidad colocar un número máximo de casos de uso o la posibilidad de colocar una bolsa de horas de monto agotable, ya que esto impide hacer un correcto dimensionamiento de la capacidad del personal que va a prestar el servicio. RTA: No se define un numero limite.
7. Se Solicita muy amablemente a la entidad indicar si para estas ubicaciones cloud o las diferentes sedes la entidad suministrara la capacidad de cómputo para colocar colectores para tomar los datos de los diferentes dispositivos. RTA: Si .
8. Se solicita muy amablemente a la entidad indicar si para el servicio de SOC se está solicitando el servicio de análisis de vulnerabilidades para los dispositivos. RTA: si se solicita
9. Se solicita muy amablemente a la entidad que tenga en cuenta que restringir el ancho de banda de la herramienta SIEM es una mala práctica, ya que puede producir retrasos en la entrega de los log y esto cause que no se pueda ver de manera oportuna un evento de seguridad. . RTA: se tendrá en cuenta.
10. Se solicita muy amablemente a la entidad aclarar a que se refieren a que se debe contar con un módulo de monitoreo de marca que proteja ante eventos externos que se puedan orquestar contra la entidad. RTA: explicación: USO INDEBIDO DE LA MARCA (Suplantación de sitio web, Registro de DNS, Suplantación de cuentas y Phising)
11. Se solicita muy amablemente a la entidad indicar si lo que está buscando son pruebas de Ética Hacking. RTA: Efectivamente las pruebas de HEC es uno de los servicios que se busca
12. SE solicita muy amablemente a la entidad indicar si requieren de una persona que configure las plataformas de la entidad para hacer la remediación de vulnerabilidades o por l contrario lo que se buscar es el acompañamiento en la configuración necesario para hacer el cierre de las vulnerabilidades, RTA: El servicio implica la identificación y reporte de vulnerabilidades, la remediación es responsabilidad propia de la entidad.
13. Se solicita a la entidad indicar si estas son las pruebas de red team a las que se refieren en el punto anterior. RTA: No es clara la pregunta.
14. Se solicita muy amablemente a la entidad modificar el ítem para permitir a oferentes que cuentan con SOC en ubicaciones con características TIER3 pero que no cuentan con su certificación. RTA: No es modificable el ítem.

15. Se solicita muy amablemente a la entidad permitir que la herramienta siem cuente con reconocimiento de otras empresas de consultaría e investigación en todo el mercado de las nuevas tecnologías. RTA: por tema contractual no es viable teniendo en cuenta que en el contrato, en las cláusulas o acuerdos de confidencialidad solo se define una empresa de consultoría.

OBSERVANTE No. 5

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
6	17/06/2022 4:53 PM	dcortes@cbtsec.com	**CROSS BORDER TECHNOLOGY**

1. Solicitamos respetuosamente a la entidad indicar de qué manera se debe hacer entrega de los logs.
2. En los numerales 15, 16 y 17 de las condiciones del servicio requerido, se describe lo siguiente: Se solicita respetuosamente a la Fiduprevisora indicar si el licenciamiento del servicio hace referencia al SOC o a la herramienta SIEM que se instalará para el funcionamiento del monitoreo y correlación de eventos. RTA: Hace referencia al SOC que implícitamente esta la herramienta SIEM.
3. En el numeral 7 de las condiciones del servicio requerido, se describe lo siguiente: Solicitamos respetuosamente a la entidad aclarar cuantas horas requiere para las capacitaciones a los funcionarios indicados. RTA: Esto depende de la complejidad y usabilidad de la plataforma, nos basaríamos en la experticia de proveedor teniendo en cuenta que después de la capacitación el acompañamiento es un factor vital para fortalecer la curva de aprendizaje.
4. Solicitamos respetuosamente a la entidad informar si tienen ANS establecidos para el cumplimiento de la ejecución de los servicios a contratar. RTA: “Responder ante cualquier falla que se llegue a materializar en la prestación del servicio y resolver en los tiempos de respuesta estipulado en los acuerdos de niveles de servicio (ANS), Realizar actividades de verificación, control y seguimiento de la calidad y niveles de servicio, con miras a permitir el monitoreo y verificación de cumplimiento de las obligaciones contractuales”
5. Solicitamos respetuosamente a la entidad indicar cuando se daría inicio con la ejecución del contrato. RTA: Desde el 01-01-2023
6. Solicitamos respetuosamente a la entidad indicar cuanto tiempo deberá estar vigente la cotización que envíen los posibles oferentes. RTA: 30 días calendario

OBSERVANTE No. 6

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
22	17/06/2022 4:12 PM	SECOP II	**ADSUM SOLUCIONES TECNOLOGICAS**

1. Se solicita de manera atenta a la entidad aclarar el alcance del servicio, “El servicio del SOC deberá contar con alta disponibilidad,” es de nuestro entendimiento que la Alta Disponibilidad se refiere a canales de contingencia por los cuales se generara la conectividad y envió de Logs desde la Fiduprevisora hasta el SOC dl oferente. RTA: Alta disponibilidad hace referencia

disposición tecnológica, técnica y humana que aseguren la verificación, control y seguimiento de la calidad y niveles de servicio, con miras a permitir el monitoreo continuo.

2. Se solicita de manera atenta a la entidad aclarar el alcance del servicio, "La solución de SIEM debe contar de forma integrada y sin necesidad de licenciamiento aparte, un módulo para la creación de nuevos recolectores para tecnología no soportada por el fabricante de forma nativa", es de nuestro entendimiento que el ítem en mención hace referencia a parcheo de Logs. RTA: Se solicita que la solución de SIEM permita la integración y monitoreo de todo tipo de tecnología, los archivos log no se parchean.

3. Se solicita aclarar a la entidad, la cantidad de equipos finales que debe soportar ya que en el numeral 3 que menciona una capacidad mínima de cuatrocientos (400) dispositivos (servidores, dispositivos de red, dispositivos de seguridad, equipos de cómputo de usuarios con privilegios de administración o cargos críticos). Favor aclarar. RTA: cantidad de equipos finales 350,

4. Se solicita de manera atenta a la entidad aclarar el alcance "La solución SIEM deberá permitir entre otros usos monitorear, detectar y tomar medidas correctivas a través de la integración nativa con elementos de seguridad en el Endpoint y en el perímetro" es de nuestro entendimiento que debe integrarse a la solución del SIEM una herramienta tipo SOAR, para respuesta automatizada a nivel del Endpoint. RTA: Es correcto.

16. Se solicita de manera atenta dentro de la implementación de nuevos casos de uso en la detección de incidentes de seguridad y ciberseguridad de la información, aclarar cuantos casos de uso máximo espera la entidad sean configurados por el oferente RTA: No se define un numero limite.

5. Se solicita de manera atenta en el ítem "La solución SIEM deberá proveer mecanismos para asegurar la integridad de los logs almacenados." Indicar la retención mínima de logs requerida. RTA: El máximo y el mínimo se definen con las TRD.

6. Se solicita de manera atenta en el ítem "El SIEM deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel, que permita revisar: inicios de sesión en los servicios en la nube, donde se registran los usuarios (incluso fuera de la red corporativa), qué actividad realizan los administradores de servicios en la nube, usuarios retirados que continúen autenticándose en los servicios." Aclarar el alcance de este servicio, es de nuestro entendimiento que requieren temas asociados a herramientas de gestión de usuarios privilegiados PAM. RTA: Alcance: "monitoreo de las aplicaciones en la nube de la entidad, utilizando como detección una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube"

7. Se solicita de manera atenta a la entidad aclarar si tienen actualmente una herramienta de gestión de usuarios privilegiados tipo PAM, que se capaz de enviar al SIEM esta información La solución SIEM debe permitir la creación de paneles y el monitoreo de actividad de usuarios privilegiados en el dominio tales como: Monitoreo del manejo de cuentas (altas, bajas, reset password, etc.); elevación de privilegios, monitoreo de cuentas de usuario VIP, monitoreo de cuentas de usuario privilegiados entre otros. Para su análisis y correlación. RTA: No se tiene

8. Se solicita amablemente a la entidad aclarar si actualmente cuentan con herramientas de uso indebido de la marca, por favor mencionar cuales, y con que software debe tener integración, para dar cumplimiento al siguiente ítem La solución SIEM debe permitir la creación de paneles y el monitoreo de actividad de usuarios privilegiados en el dominio tales como: Monitoreo del manejo de cuentas (altas, bajas, reset password, etc.); elevación de privilegios, monitoreo de

cuentas de usuario VIP, monitoreo de cuentas de usuario privilegiados entre otros. Para su análisis y correlación. . RTA: No se tiene

9. USO INDEBIDO DE LA MARCA
   - Suplantación de sitio web
   - Registro de DNS
   - Suplantación de cuentas
   - Phishing

   RTA: No hay pregunta.
10. Se solicita a la entidad si se requiere ofrecer servicio de monitoreo de integridad de archivos para servidores Windows, indicar cantidad de servidores Windows. RTA: 150
11. Se solicita a la entidad si se requiere ofrecer servicio de monitoreo de análisis de comportamiento, indicar número de agentes avanzados. RTA: 250
12. Se solicita a la entidad aclarar el ítem MODIFICACION Y/O ALTERACION NO AUTORIZADA - Modificación no autorizada de la infraestructura RTA: Monitoreo de integridad - identificación de cambios.
13. Se solicita a la entidad aclarar qué tipo de fuente de información tiene la entidad para recolectar los logs para CIBERSABOTAJE -Hacktivismo - Noticias Falsas RTA: AbuseCH, AlienVault OTX, Anomali, Cybersixgill, MISP, Recorded Future, ThreatQuotient, twitter, Facebook, Instagram, Google, duckduckgo.
14. Se solicita a la entidad aclarar qué tipo de fuente de información tiene la entidad para recolectar los logs para EXPLOTACION DE VULNERABILIDADES -Mala configuración - Sistema no actualizado RTA: SOC.
15. Se solicita a la entidad aclarar el alcance y el tipo de fuente de información que tiene la entidad para recolectar logs para ATAQUES CIBERNETICOS DIRIGIDOS -Whaling, -IngenieraSocial - SpearPhishing -AVT: Amenaza volátil avanzada, - Espionaje industrial y Robo de propiedad intelectual. RTA: SOC.
16. Se solicita aclarar en el item El servicio debe permitir correlacionar la información de accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades. Aclarar el alcance del servicio RTA: alcance: establecimiento y definición de ambientes controlados de pruebas de seguridad.
17. Se solicita en el ítem La solución SIEM debe estar en la capacidad de hacer push de scripts, como parte de las opciones de respuesta accionables. Aclarar si se puede implementar push de scripts o playbooks predefinidos para ejecutar este alcance RTA: si es posible
18. Se solicita a la entidad conocer que elemento tipo DAM cuenta la entidad para poder suministrar la siguiente información al SIEM La solución SIEM deberá contar con un módulo que permita recolectar a manera de sniffer información de sentencias transaccionales a bases de datos con el objetivo de monitorear, analizar, correlacionar y alertar estos eventos. La solución no deberá requerir modificaciones en las bases de datos a monitorear. RTA: Por supuesto que no ya que se vería afectada la confidencialidad e integridad de la información de las BD.
19. La solución SIEM debe realizar automáticamente la generación de un mapa de calor, asociándole valores de riesgo cualitativo (Alto, Medio y Bajo) a los incidentes que se están presentando en un período de tiempo determinado La solución de permitir mecanismos de búsquedas rápidas, eficientes y que permitan ser exportadas a formatos tales como *.csv.

    Se solicita eliminar o modificar este ítem ya que, ya que todas las marcas de SIEM no manejan este mismo nivel de riesgo, en estas condiciones, se solicita que la herramienta tenga un nivel

de riesgo en el cual pueda permitir búsquedas rápidas y eficientes. Contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA, OTX de Alien Vault o vinculación directa y activa con grupos de respuestas a incidentes como FIRST o similares (cualquiera de estas es válida, así como los grupos similares presentados). Especificar cuáles y contactos para revalidar alianzas. RTA: El nivel de riesgo se puede modificar ya que es cierto que "todas las marcas de SIEM no manejan este mismo nivel de riesgo", se permite que el proveedor proponga los contactos para revalidar alianzas y junto a la entidad los aprueba.

20. Se solicita Modificar parcialmente este ítem permitiendo que se pueda dar cumplimiento que el SOC pueda certificar que cuenta con procesos consolidados de gestión de incidentes en el cual se alimente de fuentes confiables a nivel mundial, manteniendo información de primera mano asociado a vulnerabilidades, amenazas, modos de explotación entre otros, con la clara intención de generar participación y pluralidad de oferentes, modificando el requerimiento de esta manera:
"Contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA, OTX de Alien Vault o vinculación directa y activa con grupos de respuestas a incidentes como FIRST o similares (cualquiera de estas es válida, así como los grupos similares presentados). Especificar cuáles y contactos para revalidar alianzas. y/o certificar que el SOC cuenta con las capacidades de manejar procesos consolidado de gestión de incidentes en el cual se alimente de fuentes confiables a nivel mundial" RTA: No se modifica teniendo en cuenta que los lineamientos definidos son los básicos para la gestión de incidentes, se permite que el proveedor proponga los contactos para revalidar alianzas y junto a la entidad los aprueba

21. Se solicita amablemente a la entidad incluir dentro del pliego una certificación emitida directamente por el fabricante donde se evidencie que el oferente se encuentra certificado en uno de los dos niveles máximos de membrecía de la solución ofertada. Esta certificación debe ser dirigida a la entidad relacionando número de proceso, no debe superar los treinta (30) días desde la fecha de expedición al cierre del proceso. ya que el nivel de membrecía permite avalar a los partners o canales sus capacidades técnicas y profesionales específicas, sobre los productos de seguridad perimetral adquiridos por la entidad. RTA: la inclusión es viable.

OBSERVANTE No. 7

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
10	17/06/2022 4:54 PM	SECOP II	**SECURESOFT**

1. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 9: Solicitamos amablemente a la entidad aclarar este ítem, puesto que la relación de cantidad de dispositivos y EPS no coinciden, ya que 500 EPS es una cantidad muy pequeña para la cantidad de dispositivos a integrar. RTA: el termino "de hasta" es el punto de partida- valor mínimo.

2. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 13: Solicitamos amablemente a la entidad aclarar si la solución a la que se refieren en este numeral es para tomar acciones de respuesta automatizada por la plataforma con un módulo de orquestación SOAR. RTA: Efectivamente es para tomar acciones de respuesta automatizada por la plataforma con un módulo de orquestación SOAR

3. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 19: Solicitamos amablemente a la entidad informar cual es la estructura de las aplicaciones a nivel de sistema operativo, adicionalmente aclarar el servicio al que se refiere este ítem y que es lo que se quiere recolectar de las aplicaciones. ¿El formato .txt, es el único formato que debería recibir la aplicación? RTA: El .txt no es el único pero si es el básico.
4. Solicitamos amablemente a la entidad informar que tipo de nube maneja la entidad, pública o privada o hibrida; a la que hace referencia el ítem 2.2 Especificaciones técnicas del servicio, numeral 21. RTA: Solo publica
5. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 27: Dado que las tecnologías de SIEM están en capacidad de recolectar los Logs de auditoria nativa que se generen dentro de los servicios de bases de datos, y no incorpora dentro de sus arquitecturas componentes de Sniffer de red. Se solicita amablemente a la entidad aclarar este numeral, ¿se requiere que el siem tenga la capacidad de leer los logs de auditoría que se almacenan dentro de los servicios de bases de datos, para correlacionar esta información con otros componentes de los servicios? RTA: La solución debe recolectar los Logs que se generen dentro de los servicios de bases de datos pero no deberá en ningún momento modificar la arquitectura ni la data de la base de datos.
6. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 66: Solicitamos amablemente a la entidad aclarar, a que hace referencia este análisis estático y dinámico dentro del servicio de Ethical Hacking RTA: el análisis de código es un proceso de revisión del código.
7. Del ítem 2.2 Especificaciones técnicas del servicio, numeral 67: Se solicita a la entidad informar con que periodicidad se realizaran estas pruebas y cuál es la cantidad de correos electrónicos a los que se realizarán las pruebas. RTA: 1 prueba por semestre – muestro de 20 funcionarios.
8. Del ítem 2.3 Condiciones del servicio requerido, numeral 28: Revisando el listado de los equipos a monitorear y realizar el análisis de vulnerabilidades. La cantidad de 500 EPS dada por la entidad en el ítem 2.2 numeral 9, no corresponden. Solicitamos amablemente a la entidad aclarar el alcance, si es a 400 equipos o a cuantos EPS sería. RTA: Los 500 eventos por segundo EPS (Eventos por Segundo) correlacionando son referentes a los eventos de seguridad de la Infraestructura TI;
9. Del ítem 2.3 Condiciones del servicio requerido, numeral 28: Solicitamos amablemente a la entidad informar cuantas IP por plataforma/equipo se van a analizar para el servicio de análisis de vulnerabilidades.". RTA: 350
10. Del ítem 2.3 Condiciones del servicio requerido, numeral 28: Solicitamos amablemente a la entidad informar cual es la cantidad de bases de datos, números de usuarios que van a ser monitoreados por el servicio, cual es el servicio de correo que tiene la entidad y que endpoint tienen actualmente. RTA: 250

OBSERVANTE No. 8

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
8	17/06/2022 7:17 PM	SECOP II	**ENTELGY**

1. Amablemente solicitamos aclarar si se aceptará la prestación de los servicios de un SOC ubicado fuera de Colombia. RTA: Por temas normativos de protección de datos personales se recomienda que este en Colombia.
2. Solicitamos de manera atenta detallar la expectativa que tiene la entidad acerca de la alta disponibilidad. RTA: Alta disponibilidad hace referencia disposición tecnológica, técnica y humana que aseguren la verificación, control y seguimiento de la calidad y niveles de servicio, con miras a permitir el monitoreo continuo
3. De forma respetuosa solicitamos aclarar la cantidad de dispositivos a monitorear, ya que no es clara la información, por ejemplo; en la especificación técnica #8 menciona "de 150 a 400 dispositivos" mientras que en la especificación técnica #3 indica "una capacidad mínima de 400 dispositivos".RTA: 350
4. Según nuestro entendimiento, la cantidad aproximada de objetivos a auditar por medio del análisis de vulnerabilidades es de 231. ¿Es correcto? ".RTA: 350
5. Realizar dos pruebas de Ethical Hacking externas (caja negra): Por favor especificar sobre cuáles (URLs, bases de datos, servidores, etc) y cuántos activos. RTA: 15
6. Realizar test de penetración interno tipo caja blanca: Por favor especificar sobre cuáles (URLs, bases de datos, servidores, etc) y cuántos activos. RTA:15
7. Realizar análisis estático y dinámico. Por favor especificar sobre cuántas aplicaciones web y la frecuencia de ejecución (por ejemplo: 1 vez al año, 2 veces al año, etc) RTA: 10 aplicaciones 1 por semestre
8. Prueba de ingeniería social. Dependiendo del tipo de prueba debe realizarse como mínimo a 20 funcionarios (objetivos específicos) o masivas a la totalidad de usuarios de correo electrónico. Por favor indicar la totalidad de usuarios de correo electrónico. RTA: 20 usuarios

OBSERVANTE No. 9

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
7	20/06/2022 10:09 PM	jose.guarnizo@comware.com.co	**COMWARE**

1. La entidad requiere sea suministrado y garantizado la prestación de los servicios de Monitoreo, detección y respuesta de Seguridad, soportado en una plataforma de tipo Next Generation - Security Information and Event Manager (SIEM).
    - El proponente debe contar con un centro de operaciones de seguridad (SOC) ubicado en la ciudad de XXXX, con capacidad de prestación de servicios en la modalidad 7x24x365.
    - El contratista deberá adjuntar a su oferta Certificación de Canal de la herramienta oferta en este punto. Dicha carta no debe tener más de 30 días de emisión contados a la fecha del cierre del presente proceso y estar dirigida a la Entidad.
      RTA: No se exige una ciudad específica para el centro de operaciones de seguridad (SOC) respecto a la certificación si aplica.
2. Herramienta de correlación de eventos de seguridad – SIEM - Especificar y Anexar Información de la Herramienta

Se requiere una solución en la modalidad de servicio de tipo Next Generation - Security Information and Event Manager (SIEM), basada en big data, que combine la gestión de registros (logs), el análisis de comportamiento de Usuarios y Entidades (UEBA) y la respuesta a incidentes de seguridad en una solución integral.
La plataforma debe estar en capacidad de recopilar volúmenes masivos de datos en tiempo real, utilizar algoritmos de aprendizaje automático (machine learning) y contar con casos de uso preinstalados para detectar amenazas avanzadas.
Los requerimientos solicitados en el presente documento deberán ser cumplidos por un solo fabricante y una única plataforma, por lo cual no se aceptan soluciones que incluyan múltiples soluciones de diferentes fabricantes para su cumplimiento.
La solución deberá soportar grandes volúmenes de datos sin afectar la estabilidad de la solución.
La plataforma al ser un SIEM de nueva generación deberá contar con características como:

- Masivamente escalable y tolerante a fallas, capaz de ingerir cientos de tbytes por día y admitir la retención de datos a largo plazo.
- Análisis de comportamiento de usuarios y entidades (UEBA) incorporado, con algoritmos de aprendizaje automático para detectar con precisión las amenazas internas y avanzadas.
- Unir eventos a lo largo del tiempo utilizando modelos de cadena de amenazas (Kill Chain) para el análisis de eventos de mayor riesgo.
- Permitir la caza de amenazas de manera rápida mediante la búsqueda en lenguaje natural.

La solución debe estar clasificada como Líder en el último Cuadrante mágico de Gartner para la gestión de eventos e información de seguridad (SIEM).
La plataforma es requerida por el tiempo de vigencia del contrato y se debe garantizar soporte 7 x 24 por parte del contratista.

3. Arquitectura y Desempeño

- La solución deberá cumplir con las siguientes características:
- Debe soportar hasta XXXX eps y XXXX usuarios de red.
- Debe ser de tipo Cloud en modalidad Software as a Service y contar con las certificaciones SOC 2 TIPO II, SOC 3, PCI-DSS e ISO 27001.
- Debe estar alojada en uno de los proveedores de nube clasificados como líder en el último Cuadrante mágico de Gartner de Servicios de infraestructura y plataforma de nube.
- Debe incluir la retención de todos los logs/eventos crudos (raw data) durante un periodo de 90 días in-line y 365 días off-line, como parte de la oferta.
- Debe incluir la retención de todos los eventos procesados (alertas, desviaciones, modelamientos) durante por un periodo de 90 días in-line y 365 días off-line, como parte de la oferta básica sin que esto represente un costo adicional.
- Debe incluir una herramienta de Security Datalake integrada, basada en Bigdata y con capacidad de colectar, consumir y almacenar los datos por periodos establecidos en este pliego, para efectos de cumplimiento e investigación, como parte de la oferta.
- Debe incluir un esquema de alta disponibilidad y de recuperación ante desastres. La solución debe contar con esquemas de alta disponibilidad en cada uno de sus componentes de procesamiento de los datos.

El esquema de recuperación de desastres incluido debe contar como mínimo con un ambiente de recuperación ante desastres en frío, geográficamente distanciado del ambiente principal, que se iniciará durante un desastre y donde se restaura una copia de seguridad a este entorno en caso de una declaración de desastre.
El esquema de recuperación de desastres incluido debe contar como mínimo con un esquema de copias de seguridad con diario para los datos y por hora para las configuraciones.

- Se debe incluir como parte de la oferta un esquema del mantenimiento de rutina y las actualizaciones del ambiente para garantizar un servicio confiable y la máxima disponibilidad.
- La solución debe contar con una arquitectura "Multitenencia" o multi-tenancy, que permita la separación lógica de los datos de diferentes clientes.
- Debe permitir el filtrado y la compresión de los datos selectivos en hasta un 90% en el punto de recolección.
- Debe permitir la gestión de ancho de banda para la transmisión de los datos entre la capa de recolección y la de análisis.
- Debe realizar caché local y/o almacenamiento en búfer en los puntos de recolección de los datos (colector) para garantizar que no se pierdan datos en tránsito en caso de un problema de red o un pico en el volumen de eventos.
- Debe garantizar un enfoque de defensa en profundidad para la seguridad. Este enfoque limita el acceso ambiente y aplica el privilegio de mínimo acceso, adecuado a la infraestructura.
  Debe admitir cifrado de datos transparente (TDE) de extremo a extremo. Transparente significa que los usuarios finales no deben percibir los procesos de cifrado / descifrado, y de extremo a extremo que los datos se cifran tanto en reposo como en tránsito.
  Debe admitir enmascaramiento de datos a través de controles de acceso granulares basados en roles, para ofuscar cualquier información potencialmente confidencial de los usuarios en la capa de la interfaz de usuario.
  Debe admitir control de acceso basado en roles granulares (RBAC) con soporte para administración delegada, tanto a las funcionalidades en la interfaz de usuario como también a los datos a los que puede.
  La solución debe contar con un sistema de administración para las llaves de cifrado incluido y que permita la rotación de las mismas con una base de un año.
- La solución debe poder acceder a través de la Internet pública, incluyendo tanto la consola como los servicios web API.
- La solución debe ser accesible únicamente a través del puerto HTTPS y contar con un certificado digital vigente y expedido por una entidad certificadora externa que garantice la identidad del sitio.

4. Ingestión

- La solución deberá cumplir con las siguientes características:
- Debe soportar la integración con más de 500 fuentes de terceros mediante los métodos syslog, formatos de registros estructurados (CEF, LEEF, MEF, JSON, XML), archivos, bases de datos, (conexión JDBC), conexión API (e.g., AWS Cloudwatch, AWS Cloud Trail, AWS EKS, Bitglass, Azure Log Analytics, Azure reports, Azure msftgraphsecurity, Box, Carbon

Black, Cisco ISE, Cisco Umbrella, Cloudera, CrowdStrike, Cylance, Dropbox, DUO, Google Report, Google big query, Google Directory, Netskope, Netwitness, Office365, Okta, Proof point, Qradar API Connector, SVN, Salesforce, SentinelONE, Sophos, Symantec, SureView, Workday, zoom), WMI, consultas LDAP/LDAPS, datos de flujos (e.g., Netflow, sFlow, jFlow), Hadoop, listener, registros no estructurados (REGEX Builder), agentes de terceros (e.g., Snare).

- Debe permitir la integración con diferentes tipos de fuentes de datos como datos de indentidad, logs de actividad/transacciones, logs de eventos de seguridad, flujos de red, logs de aplicaciones/plataformas cloud, permisos de acceso, fuentes de inteligencia de amenazas, data no estructurada, metadata de activos.
- Debe integrarse con sistemas externos de gestión de identidades y/o IAM como Active Directory/LDAP, Azure Active Directory, Google, Okta, Oracle IDM, Oracle Indentity Analytics (OIA), Salesforce, SailPoint, Waveset, bases de datos o archivos, entre otros, y realizar enriquecimiento de los eventos agregando la identidad del usuario en cada uno de los eventos colectados.
- Debe estar en al capacidad de conectarse de forma nativa a través de APIs u otros medios con servicios cloud como AWS Cloudwatch, AWS Cloud Trail, AWS EKS, Bitglass, Azure Log Analytics, Azure reports, Azure msftgraphsecurity, Box, Carbon Black, Cisco ISE, Cisco Umbrella, Cloudera, CrowdStrike, Cylance, Dropbox, DUO, Google Report, Google big query, Google Directory, Netskope, Netwitness, Office365, Okta, Proof point, Qradar API Connector, SVN, Salesforce, SentinelONE, Sophos, Symantec, SureView, Workday, Zoom, ServiceNow, entre otros.
- Debe contar con una interfaz de usuario que permita modificar conectores/parseadores existentes o construir nuevos parseadores directamente desde la misma interfaz de usuario UI.
- Debe contar con conectores/parseadores preconfigurados listos para usar, pero que se puedan modificar según sea necesario. El parseo, normalización y categorización de los colectores deben ser totalmente personalizables desde la interfaz de usuario.
- Debe contar con una API RESTful de servicios web abiertos y disponible en internet para la integración bidireccional con otras tecnologías.
- Debe proporcionar integración con al menos 10 fuentes de inteligencia de amenazas sin costo adicional.
- Debe contar con una funcionalidad de autodescubrimiento de fuentes de datos basadas en syslog que simplifique y automatice el proceso de integración.
- Debe realizar enriquecimiento contextual de datos sobre los eventos agregando la identidad de usuario, contexto de negocio, metadatos de activos, información de red, ubicación geográfica y datos de inteligencia de amenazas sobre los eventos en el momento de la captura/ingestión.
- Debe enriquecer los eventos en tiempo real con el contexto de usuario y entidad. Los datos enriquecidos deben proporcionar atributos de contexto que se pueden utilizar para la elaboración de perfiles de comportamiento, comparaciones entre pares y búsquedas e investigaciones.

5. Analítica Avanzada de Seguridad

- La solución deberá cumplir con las siguientes características:
- Debe detectar amenazas internas y cibernéticas avanzadas mediante el uso de aprendizaje automático (machine learning) para perfilar y crear líneas base de comportamiento de usuarios y entidades.
- Debe proporcionar contenido listo para usar que incluya conectores, parsers, políticas y modelos de amenazas. Las políticas y los modelos de amenazas deben estar clasificados por funcionalidad.
- Debe contar con contenido pre empaquetado de casos de uso y modelos de amenazas listos para usar para la detección avanzada de amenazas, como amenazas internas, uso indebido de privilegios, amenazas cibernéticas, análisis de seguridad en la nube, análisis de seguridad de aplicaciones, análisis de identidad y acceso y fraude.
- Debe analizar los registros en tiempo real utilizando una combinación de diferentes técnicas de análisis y algoritmos.
- Debe contar con diferentes técnicas de análisis como perfiles de comportamiento, análisis de pares y grupos, inteligencia de negocio y de amenazas y modelado de amenazas.
- Debe proporcionar capacidades integrales para modelar y ajustar la puntuación de riesgo según el perfil del usuario y/o entidad, la gravedad de la amenaza y la secuencia/combinación de eventos que ocurren durante un período de tiempo.
- Debe permitir el modelado de riesgos desde la interfaz de usuario según las prioridades de la organización.
- Debe contar con modelos de amenazas que permitan agrupar eventos realizados por un usuario o entidad que abarque días, semanas, meses, etc. Estas actividades se deben mostrar en la UI en forma de kill chain con cada evento categorizado en etapas predefinidas.
- Debe contar con algoritmos predictivos para identificar a los usuarios riesgosos (por ejemplo, usuarios a punto de abandonar la organización).
- Debe proporcionar análisis para diferentes tipos diferentes de anomalías como tiempo relacionado, volumen de transferencia de datos, fuente de eventos relacionados, evento-destino relacionado, anomalías por usuario y grupo de pares, anomalías relacionadas con la ubicación geográfica / velocidad terrestre, así como también rastrear usuarios u otras entidades en listas de monitoreo.
- Debe disponer de algoritmos de aprendizaje no supervisado para analizar eventos actuales e históricos y determinar asociaciones, para establecer patrones de comportamiento de la actividad del usuario en cada fuente de eventos por día, semana, mes, hora del día y día de la semana. Cualquier desviación del patrón regular se debe marcar como una anomalía.
- Debe disponer de algoritmos de aprendizaje supervisado para detectar amenazas avanzadas de malware como DGA, ataques de phishing / SPAM, etc.
- Debe disponer de técnicas de análisis basadas en pares para detectar usuarios que comienzan a comportarse de manera distinta a los pares, perfilando el comportamiento

de los diferentes usuarios en el grupo de pares y luego comparando las transacciones del usuario con las de los pares.

- Debe disponer de técnicas de análisis de rareza de eventos mediante el cual se identifiquen actividades sospechosas que no han sido vistas antes.
- Debe disponer de técnicas de análisis de comportamiento por enumeración que permitan crear líneas base de eventos del mismo tipo y buscar cualquier desviación de lo normal.
- Debe disponer de técnicas de análisis de tráfico para identificar patrones de beaconing, agentes de usuario inusuales, conexión a URLs inusuales, conexiones a dominios DGA, etc.
- Debe disponer de técnicas de análisis de datos de ubicación geográfica para buscar patrones de inicio de sesión que indiquen el potencial intercambio/compromiso de la identidad del usuario. Por ejemplo, distintos inicios de sesión de un usuario desde diferentes países en un periodo de tiempo muy corto.
- Debe proporcionar la capacidad de definir políticas basadas en reglas para detectar amenazas conocidas. Estas amenazas conocidas deben utilizarse como potenciadores de riesgos y combinados con los análisis “sin firma” en los modelos de amenazas.
- Debe contar con modelamiento de amenazas que permita identificar amenazas compuestas, que si se observan de forma aislada pueden ser de bajo riesgo, sin embargo, cuando se combinan, son un indicio de un evento de alto riesgo.
- Debe reducir el número de falsos positivos al aplicar capacidades avanzadas de aprendizaje automático (machine learning) para aprender lo que es normal y no normal en el entorno.

6. Respuesta a incidentes y threat hunting

- La solución deberá cumplir con las siguientes características:
- Debe contar con un sistema de administración de casos integrado, con flujos de trabajo listos para usar que se pueden personalizar fácilmente según las necesidades específicas del cliente.
- Debe proporcionar control basado en roles dentro del flujo de trabajo para apoyar la segregación de incidentes y casos.
- Deberá tener la capacidad de integrarse con sistemas de tickets externos en caso de que la entidad lo requiera.
- Debe tener incorporado un marco de respuesta automatizado con playbooks listos para usar según el tipo de incidente. Los playbooks deben permitir a los usuarios obtener contexto y tomar medidas correctivas.
- Debe disponer de modelos de inteligencia artificial para el análisis de elecciones históricas de las acciones de los usuarios y proporcionar acciones recomendadas de remediación a los analistas, basadas en el aprendizaje del comportamiento histórico del analista.
- Debe soportar la integración con soluciones de orquestación, automatización y respuesta de seguridad de terceros.

- Debe proporcionar a los analistas capacidades de búsqueda y cacería a través de un motor de consultas flexibles de forma libre sobre millones de registros y con capacidad de respuesta de milisegundos.
- Debe incluir como parte de la oferta un entorno "sandbox" de pruebas o ambiente de desarrollo, que permita aislar del ambiente de producción nuevas integraciones, nuevos desarrollos de contenido y/o de nuevos parsers o cualquier cambio sobre estos, antes de su despliegue.
  El módulo de "Sanbox" o pruebas debe estar totalmente integrado en la misma solución, de modo que lo realizado en él pueda ser promovido al ambiente de producción fácilmente. No se acepta la implementación de tenants o nodos adicionales, separados o desagregados y que requieran de procesos adicionales para migrar lo configurado en el ambiente de pruebas al ambiente de producción.
  El módulo de "Sanbox" o pruebas debe estar totalmente integrado en la misma solución, lo que implica que desde la misma consola se debe poder visualizar y gestionar todas las desviaciones del entorno pruebas para experimentar, ajustar y desarrollar infracciones de políticas.
  Las desviaciones en el entorno de pruebas deben estar completamente aisladas de ambiente de producción, lo que significa que cualquier acción realizada para una desviación del entorno de pruebas no afecta las de producción ni contribuye a las puntuaciones de riesgo.

7. Visualización y Reportes

La solución deberá contar con las siguientes características de visualización y reportes:

- Debe disponer de reportes de amenazas que brinden visibilidad sobre la postura ante amenazas. Por ejemplo: usuarios de alto riesgo, activos de alto riesgo, principales amenazas, principales IP maliciosas, etc.
- Debe disponer de reportes que binden visibilidad de la gestión de incidentes de seguridad. Por ejemplo: estadísticas sobre incidentes abiertos / en progreso / cerrados, mientras tanto para responder (MTR), etc.
- Debe disponer de reportes que brinden visibilidad a los clientes sobre las operaciones de seguridad. Por ejemplo, para dispositivos VPN, los informes incluirían las mejores sesiones VPN por duración, los principales eventos de salida de datos, la distribución de los eventos de inicio de sesión por geografía, los principales intentos fallidos de inicio de sesión, etc.
- Debe disponer de reportes de cumplimiento alineados con requisitos de cumplimiento específicos como PCI, SOX, HIPPA, GDPR, ISO27002, etc.
- Debe disponer de reportes de resumen ejecutivo de violaciones, incidentes y operaciones.
- Debe disponer de reportes sobre la actividad de los usuarios.
- Debe permitir la visualización de los datos con diferentes tipos de gráficos: gráfico de líneas, gráfico de barras, gráfico circular, mapa geográfico, tablas, gráficos apilados, gráficos superiores N, gráficos de burbujas, gráficos de relaciones de origen-destino.

- Debe permitir la visualización de datos mediante enlaces que permitan vincular cualquier conjunto de atributos y visualizar la relación entre ellos (por ejemplo, origen, destino, puertos).

RTA: Es correcto el entendimiento.

"Defensoría del Consumidor Financiero: Dr. JOSÉ FEDERICO USTÁRIZ GÓNZALEZ. Carrera 11 A No 96-51 - Oficina 203, Edificio Oficity en la ciudad de Bogotá D.C. PBX 6108161 / 6108164, Fax: Ext. 500. E-mail: defensoriafiduprevisora@ustarizabogados.com de 8:00 am - 6:00 pm, lunes a viernes en jornada continua". Las funciones del Defensor del Consumidor son: Dar trámite a las quejas contra las entidades vigiladas en forma objetiva y gratuita. Ser vocero de los consumidores financieros ante la institución. Usted puede formular sus quejas contra la entidad con destino al Defensor del Consumidor en cualquiera agencia, sucursal, oficina de corresponsalía u oficina de atención al público de la entidad, asimismo tiene la posibilidad de dirigirse al Defensor con el ánimo de que éste formule recomendaciones y propuestas en aquellos aspectos que puedan favorecer las buenas relaciones entre la Fiduciaria y sus Consumidores. Para la presentación de quejas ante el Defensor del Consumidor no se exige ninguna formalidad, se sugiere que la misma contenga como mínimo los siguientes datos del reclamante: 1. Nombres y apellidos completos 2. Identificación 3. Domicilio (dirección y ciudad) 4. Descripción de los hechos y/o derechos que considere que le han sido vulnerados. De igual forma puede hacer uso del App "Defensoría del Consumidor Financiero" disponible para su descarga desde cualquier smartphone, por Play Store o por App Store.