NO. SOLICITUD:	**BA-CCC-LPN-2021-0006**	**OBJETO DE LA CONTRATACION:**	**Ciberseguridad Interna y Perimetral del Banco Agrícola.**
RUBRO:	**2.6.1.3.01: Seguridad de los computares, redes o internet**	**PLANIFICADA:**	Si

	SEGURIDAD INTERNA Y PERIMETRAL
1	***SEGURIDAD PERIMETRAL EMPRESARIAL EXTERNO***
1.1	La solución debe entregar un rendimiento de Firewall de al menos 32 Gbps, IPS 7.8 Gbps, NGFW 6 Gbps y Threat Protection 5 Gbps
1.2	La solución debe soportar 4 Millones de sesiones concurrentes (TCP)
1.3	La solución debe soportar nuevas sesiones / segundo (TCP) 450.000
1.4	La solución debe soportar sin necesidad de licenciamiento al menos 2,000 túneles VPN IPsec P2P
1.5	La solución debe soportar sin necesidad de licenciamiento al menos 50,000 túneles VPN IPsec de cliente a puerta de enlace
1.6	La solución debe consistir en una plataforma de protección de red, basada en un dispositivo con funcionalidades de Firewall e IPS de Próxima Generación (NGIPS y NGFW), así como consola de gestión y monitoreo.
1.7	Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
1.8	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7
1.9	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
1.10	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding
1.11	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente
1.12	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3
1.13	Tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios
1.14	Implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD

1.15	La solución debe soportar VPN de sitio-a-sitio y cliente-a-sitio
1.16	La solución debe soportar VPN IPSec
1.17	La solución debe soportar VPN SSL
1.18	La VPN IPSec debe ser compatible con 3DES
1.19	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA256, SHA384 y SHA512
1.20	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y desde Grupo 14 hasta Grupo 32
1.21	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2)
1.22	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard)
1.23	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI
1.24	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting
1.25	La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web
1.26	Las características de VPN SSL se deben cumplir con o sin el uso de agentes
1.27	La solución debe soportar la asignación de DNS en la VPN de cliente remoto
1.28	Debe permitir la creación de políticas de NGIPS, NGFW, antivirus y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL
1.29	La solución debe soportar la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local
1.30	La solución debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL
1.31	La solución debe incluir 1x USB Port
1.32	La solución debe incluir 1x Console Port
1.33	La solución debe incluir 16x GE RJ45 Ports
1.34	La solución debe incluir 16x GE SFP Slot Ports
1.35	La solución debe de ser factor forma Rack Mount, 1 RU
1.36	Debe incluir licencia de NGIPS

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

1.37	Debe incluir licencia de NGFW
1.38	Debe incluir licencia de protección avanzada contra virus
1.39	Debe incluir 4 transceiver a 1GB SFP, como también los cable de fibras de 5M a 10M.
1.40	Incluir al menos cuatros (4) cables de cobres de 5M a 10M.
1.41	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
1.42	**Dos (2) Firewalls** de última generación o **NGFW** (ambos instalados en el perímetro de la red empresarial de Banco Agrícola) e instalados bajo el esquema de alta disponibilidad (HA). Estos equipos deberán ser de una Marca diferente a la propuesta en la 4.2 del ITEM I SEGURIDAD INTERNA Y PERIMETRAL. Bajo un diseño de seguridad de red perimetral de NGFW Back-to-Back.
2	***SEGURIDAD PERIMETRAL EMPRESARIAL INTERNO***
2. 1	**Dos (2) Firewalls** de última generación o **NGFW** (ambos instalados en el perímetro de la red empresarial de Banco Agrícola) e instalados bajo el esquema de alta disponibilidad (HA). Estos equipos deberán ser de una Marca diferente a la propuesta en la 4.1 del ITEM I SEGURIDAD INTERNA Y PERIMETRAL. Bajo un diseño de seguridad de red perimetral de NGFW Back-to-Back.
2.2	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Firewall.
2.3	La solución propuesta debe ser un equipo dedicado solo para estos fines.
2.4	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro de la red empresarial.
2.5	La solución debe entregar un rendimiento de Firewall de al menos 3 Gbps, NGFW de 2.3 Gbps y NGIPS 2.3 Gbps.
2.6	Contar con 12 interfaces de red Ethernet (RJ45) y 4 x SFP integrada.
2.7	Incluir ocho (8) transceiver a 1000BASE-SX para las interfaces SFP integradas. Como también los cables de fibras de 5M a 10M.
2.8	Soportar un mínimo de sesiones simultáneas, con AVC de un (1) millón.
2.9	Soportar un mínimo de nuevas conexiones por segundo, con AVC de 14K.
2.10	Entregar un rendimiento de inspección de trafico cifrado (TLS) de 365 Mbps.

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

2.11	Contar con al menos una interfaz dedicada para la administración del hardware.
2.12	Contar con al menos un puerto serial o consola de administración.
2.13	Debe ser 1 Rack Unit.
2.14	Deber permitir establecer un total de 200 usuarios de VPN de Acceso Remoto SSL o IPSec.
2.15	La solución debe tener la capacidad de administración local.
2.16	La solución debe ser capaz de ser administrada de forma centralizada, que entregue una configuración, registro (Logging), la supervisión (monitoring) y los informes (report) de forma centralizado.
2.17	Incluir solución de administración centralizada del mismo fabricante con la capacidad de administrar un mínimo de diez (10) equipo de seguridad (NGFW).
2.18	La solución de administración ofertada puede ser virtual o físico. De ser virtual, la misma debe soportar ambiente de Microsoft Hyper-V.
2.19	La solución de administración centralizada deber tener la capacidad de correlacionar eventos de seguridad de los equipos de seguridad (NGFW) integrado a la plataforma.
2.20	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y otro) desde cualquier equipo conectado a la red que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox, Chrome) instalado sin necesidad de instalación de ningún software adicional.
2.21	Capacidad de correlacionar todos los eventos de intrusión con un impacto del ataque, y entregar al operador qué necesita atención inmediata.
2.22	La solución debe poder entregar un perfilamiento de seguridad de los hosts (IP) de la red, a través del descubrimiento de dispositivos pasivos, incluido el sistema operativo, las aplicaciones de cliente y servidor, las vulnerabilidades, el procesamiento de archivos y los eventos de conexión, etc.
2.23	Habilidad de adaptación automática de las defensas a los cambios dinámicos en la red, en archivos o con hosts. Esto debe cubrir ajuste de reglas de NGIPS y la política de firewall de red.
2.24	Habilidad de correlacionar las actividades de la red y de los hosts (dispositivos finales) mediante más de 1,000 indicadores de compromisos basado en comportamiento.
2.25	La solución debe proporcionar análisis y protección de amenazas contextuales completos, con conocimiento de los usuarios, historial de usuarios en cada máquina, dispositivos móviles, aplicaciones del lado del cliente, sistemas operativos, vulnerabilidades y amenazas.
2.26	La funcionalidad de IPS de próxima generación debe contar con conciencia contextual en tiempo real y mapeo de red.

SECCION DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

2.27	La solución ofertada debe de ser capaz de hacer recomendaciones de políticas de NGIPS para garantizar de forma correcta los ajustes de las reglas de detección y prevención de intruso.
2.28	Debe de ser capaz de realizar análisis continuo y retrospección de archivo o detección, más allá del horizonte de eventos (punto en el tiempo).
2.29	Habilidad de detectar, alertar, rastrear, analizar y remediar de manera retrospectiva el código malicioso (malware) avanzado que al principio puede parecer limpio o que evade las defensas iniciales y luego se identifica como malicioso.
2.30	Capacidad de mapear cómo los hosts transfieren archivos, incluidos los archivos de malware, a través de su red.
2.31	Habilidad para ver si se bloqueó la transferencia de un archivo o si el archivo se puso en cuarentena. Que permita proporcionar un medio para determinar el alcance, proporcionar controles de brotes e identificar al paciente cero.
2.32	Incluir sandboxing dinámicas integradas.
2.33	Habilidad de comprender, analizar y contener rápidamente un ataque activo incluso después de que suceda.
2.34	Debe ser posible obtener una visualización completa del alcance de una amenaza o ataque ya exitoso, como también contener, bloquear o poner en cuarentena.
2.35	Permita implementar políticas de seguridad de cumplimiento de acuerdo con criterios, como sistema operativo, aplicaciones (Web y Cliente) y protocolos de red.
2.36	Capacidad de realizar línea base (base line) de tráfico de la red de acuerdo con definición de la red, host, servicio, otros.
2.37	Permita tomar acciones de acuerdo con los eventos de violaciones de cumplimientos.
2.38	Contar con reportes predefinidos por el fabricante.
2.39	Permitir crear o personalizar reporte de seguridad y red, de acuerdo a malware, aplicaciones, intrusión, etc.
2.40	Permitir descargar o exportar los reportes de seguridad generado en la solución.
2.41	Permitir enviar reportes de seguridad a un repositorio externo.
2.42	Permitir almacenar reportes de seguridad de forma local.
2.43	Debe entregar los reportes en formato de archivo de al menos PDF, HTML y CSV.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

2.44	El Threat Intelligence propuesto debe ser del mismo fabricante de la solución propuesta.
2.45	Debe contar con Inteligencia de amenazas e interdicción, Investigación de detección, Ingeniería y desarrollo, Investigación y descubrimiento de vulnerabilidades, Comunidades, Alcance global y Repuesta a Incidente directamente del Centro de Inteligencia de Amenazas de la solución propuesta.
2.46	Capacidad de enviar alerta vía SNMP, Syslog y correo electrónico.
2.47	Debe enviar alertas de eventos de intrusión, tales como: - El host de origen o destino está potencialmente comprometido por un virus, un troyano u otra pieza de software malicioso. - El host de origen o destino está en la red y se establece una vulnerabilidad al host - Entre otros.
2.48	Poder enviar alertas de acuerdo con parámetros de redes, tales como: cliente, host, puerto, protocolo, entre otros.
2.49	Capacidad de enviar alertas de eventos de malware.
2.50	Permitir al operador especificar de forma granular las alertas de amenazas a recibir vía correo electrónico, es decir, especificar cuáles reglas de NGIPS desea recibir las alertas.
2.51	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
2.52	Garantizar el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento.
2.53	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
3	***SEGURIDAD PERIMETRAL PARA CENTRO DE DATOS***
3.1	**Dos (2) IPS** de última generación o **NGIPS** (ambos instalados en el perímetro de la red del Centro de Dato Principal de Banco Agrícola) e instalados bajo el esquema de alta disponibilidad (HA). Estos equipos deberán ser de una Marca diferente a la propuesta en la 4.1 del ITEM 3 SEGURIDAD INTERNA Y PERIMETRAL.
3.2	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de IPS.

3.3	La solución propuesta debe ser un equipo dedicado solo para estos fines.
3.4	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.
3.5	La solución debe entregar un rendimiento de firewall de 10 Gbps, NGFW de 5 Gbps y NGIPS 5 Gbps.
3.6	Contar con 12 x 10M/100M/ 1GBASE-T interfaces Ethernet (RJ- 45) y 4 x 10 Gigabit (SFP+) interfaces Ethernet integrada.
3.7	Incluir ochos (8) transceiver 10GBASE-SR SFP Module, como también los cables de fibras de 5M a 10M.
3.8	Soportar un mínimo de sesiones simultáneas, con AVC de dos (2) millones.
3.9	Soportar un mínimo de nuevas conexiones por segundo, con AVC de 27K.
3.10	Entregar un rendimiento de inspección de trafico cifrado (TLS) de 735 Mbps.
3.11	Contar con módulo de Fail-to-Wired que incluya al menos seis (6) interfaces a 10Gbps SR.
3.12	Incluir fuente de corriente redundante.
3.13	Contar con al menos una interfaz dedicada para la administración del hardware.
3.14	Contar con al menos un puerto serial o consola de administración.
3.15	Debe ser 1 Rack Unit.
3.16	La solución debe tener la capacidad de administración local.
3.17	La solución debe ser capaz de ser administrada de forma centralizada, que entregue una configuración, registro (Logging), la supervisión (monitoring) y los informes (report) de forma centralizado.
3.18	Incluir solución de administración centralizada del mismo fabricante con la capacidad de administrar un mínimo de diez (10) equipo de seguridad (NGFW/NGIPS).
3.19	La solución de administración ofertada puede ser virtual o físico. De ser virtual, la misma debe soportar ambiente de Microsoft Hyper-V.
3.20	La solución de administración centralizada deber tener la capacidad de correlacionar eventos de seguridad de los equipos de seguridad (NGFW) integrado a la plataforma.
3.21	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y otro) desde cualquier equipo conectado a la red que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox, Chrome) instalado sin necesidad de instalación de ningún software adicional.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

3.22	Capacidad de correlacionar todos los eventos de intrusión con un impacto del ataque, y entregar al operador qué necesita atención inmediata.
3.23	La solución debe poder entregar un perfilamiento de seguridad de los hosts (IP) de la red, a través del descubrimiento de dispositivos pasivos, incluido el sistema operativo, las aplicaciones de cliente y servidor, las vulnerabilidades, el procesamiento de archivos y los eventos de conexión, etc.
3.24	Habilidad de adaptación automática de las defensas a los cambios dinámicos en la red, en archivos o con hosts. Esto debe cubrir ajuste de reglas de NGIPS y la política de firewall de red.
3.25	Habilidad de correlacionar las actividades de la red y de los hosts (dispositivos finales) mediante más de 1,000 indicadores de compromisos basado en comportamiento.
3.26	La solución debe proporcionar análisis y protección de amenazas contextuales completos, con conocimiento de los usuarios, historial de usuarios en cada máquina, dispositivos móviles, aplicaciones del lado del cliente, sistemas operativos, vulnerabilidades y amenazas.
3.27	La funcionalidad de IPS de próxima generación debe contar con conciencia contextual en tiempo real y mapeo de red.
3.28	La solución ofertada debe de ser capaz de hacer recomendaciones de políticas de NGIPS para garantizar de forma correcta los ajustes de las reglas de detección y prevención de intruso.
3.29	Debe de ser capaz de realizar análisis continuo y retrospección de archivo o detección, más allá del horizonte de eventos (punto en el tiempo).
3.30	Habilidad de detectar, alertar, rastrear, analizar y remediar de manera retrospectiva el código malicioso (malware) avanzado que al principio puede parecer limpio o que evade las defensas iniciales y luego se identifica como malicioso.
3.31	Capacidad de mapear cómo los hosts transfieren archivos, incluidos los archivos de malware, a través de su red.
3.32	Habilidad para ver si se bloqueó la transferencia de un archivo o si el archivo se puso en cuarentena. Que permita proporcionar un medio para determinar el alcance, proporcionar controles de brotes e identificar al paciente cero.
3.33	Incluir sandboxing dinámicas integradas.
3.34	Habilidad de comprender, analizar y contener rápidamente un ataque activo incluso después de que suceda.
3.35	Debe ser posible obtener una visualización completa del alcance de una amenaza o ataque ya exitoso, como también contener, bloquear o poner en cuarentena.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

3.36	Permita implementar políticas de seguridad de cumplimiento de acuerdo con criterios, como sistema operativo, aplicaciones (Web y Cliente) y protocolos de red.
3.37	Capacidad de realizar línea base (base line) de tráfico de la red de acuerdo con definición de la red, host, servicio, otros.
3.38	Permita tomar acciones de acuerdo con los eventos de violaciones de cumplimientos.
3.39	Contar con reportes predefinidos por el fabricante.
3.40	Permitir crear o personalizar reporte de seguridad y red, de acuerdo a malware, aplicaciones, intrusión, etc.
3.41	Permitir descargar o exportar los reportes de seguridad generado en la solución.
3.42	Permitir enviar reportes de seguridad a un repositorio externo.
3.43	Permitir almacenar reportes de seguridad de forma local.
3.44	Debe entregar los reportes en formato de archivo de al menos PDF, HTML y CSV.
3.45	El Threat Intelligence propuesto debe ser del mismo fabricante de la solución propuesta.
3.46	Debe contar con Inteligencia de amenazas e interdicción, Investigación de detección, Ingeniería y desarrollo, Investigación y descubrimiento de vulnerabilidades, Comunidades, Alcance global y Repuesta a Incidente directamente del Centro de Inteligencia de Amenazas de la solución propuesta.
3.47	Capacidad de enviar alerta vía SNMP, Syslog y correo electrónico.
3.48	Debe enviar alertas de eventos de intrusión, tales como: - El host de origen o destino está potencialmente comprometido por un virus, un troyano u otra pieza de software malicioso. - El host de origen o destino está en la red y se establece una vulnerabilidad al host - Entre otros.
3.49	Poder enviar alertas de acuerdo con parámetros de redes, tales como: cliente, host, puerto, protocolo, entre otros.
3.50	Capacidad de enviar alertas de eventos de malware.
3.51	Permitir al operador especificar de forma granular las alertas de amenazas a recibir vía correo electrónico, es decir, especificar cuáles reglas de NGIPS desea recibir las alertas.

3.52	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
3.53	Garantizar el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento.
3.54	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
4	***SEGURIDAD DE CORREO ELECTRONICO***
4.1	Solución SaaS con integración nativa a través de APIs con Microsoft Office 365.
4.2	La solución debe integrarse con Microsoft Exchange en la premisa de la institución.
4.3	La solución debe tener la capacidad de detener amenazas de email para correos entrantes y salientes.
4.4	Capacidad de combatir el ransomware oculto en archivos adjuntos que evaden la detección inicial de la infraestructura de seguridad.
4.5	La solución debe tener la capacidad de entregar protección a 850 buzones o cuentas de correos electrónicos.
4.6	La solución debe de proteger el contenido sensible en los correos electrónicos salientes con Prevención de pérdida de datos (DLP).
4.7	Capacidad de responder de forma proactiva a las amenazas cibernéticas, como malware, spam, ransomware, ataques de phishing y ataques dirigidos.
4.8	La solución no debe requerir el cambio de los registros MX para la integración en Office365.
4.9	Incluir protección Antimalware con validación de reputación de archivos y análisis de malware.
4.10	Capacidad de remediar de forma automática mensajes con contenido malicioso.
4.11	La solución debe poder eliminar automáticamente los correos electrónicos con enlaces peligrosos.
4.12	La solución debe permitir visualizar la trayectoria y conversaciones de los mensajes
4.13	La solución debe contar con una herramienta de Respuesta a amenazas donde se pueda realizar Threat Hunting de forma nativa.
4.14	Capacidad de bloquear el acceso a sitios recientemente infectados con análisis de URL en tiempo real para proteger contra el phishing y correo comprometidos.

4.15	Capacidad de modelar el comportamiento de las amenazas de apropiación de cuentas para bloquear ataques que se originan en cuentas de correo electrónico comprometidas.
4.16	La solución debe tener la capacidad de bloquear correos electrónicos no deseados con filtrado de reputación.
4.17	Poseer una arquitectura de escaneo de correos electrónicos no deseados de múltiples capas de seguridad.
4.18	Poseer funcionalidad de análisis adaptable al contexto del correo electrónico, es decir, examina el contexto completo de un mensaje, incluido el contenido del mensaje, cómo se construye el mensaje, quién envía el mensaje y otros.
4.19	Capacidades de tomar acciones de acuerdo con el contexto del correo electrónico.
4.20	Capacidad de detección y control de correos electrónicos de publicidad.
4.21	Capacidad de bloqueo de URL maliciosas con filtrado de URL según la reputación o la categoría de las URL.
4.22	Capacidad de entregar al operador la de realizar un seguimiento de los usuarios finales que hacen clic en las URL maliciosas.
4.23	La solución debe ser capaz de realizar DLP que evite que los datos confidenciales salgan de la institución.
4.24	Poseer una amplia biblioteca de políticas predefinidas de DLP de al menos 100 políticas que cubran regulaciones gubernamentales y específicas de la empresa.
4.25	Contar con políticas de DLP predefinidas y simplifique la aplicación de la política de correo electrónico saliente con reconocimiento de contenido.
4.26	Incluir funcionalidad de DLP que abarque la remediación o corrección que incluyen cifrado, agregar pies de página y exenciones de responsabilidad, agregar copias carbón ocultas (BCC), notificar y poner en cuarentena, otros.
4.27	Proveer capacidades de detección y bloqueo de malware con puntuación y bloqueo de reputación de archivos, sandboxing y retrospección de archivos para un análisis continuo de amenazas, incluso después de que hayan atravesado la puerta de enlace de correo electrónico.
4.28	Capacidad de realizar filtrado de la reputación de IP del remitente que apoye en la protección contra correo no deseado.
4.29	Capacidad de consumir informaciones de amenazas externas en formato STIX comunicada a través del protocolo TAXII.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

4.30	Capacidad de proporcionar un veredicto de reputación para los mensajes de correo electrónico según el dominio del remitente y otros atributos.
4.31	Capacidad de proporcionar una vista segura (versión PDF impresa segura) de un archivo adjunto de mensaje detectado como malicioso o sospechoso al usuario final.
4.32	La solución debe incluir motores de detección de virus integrados de marcas reconocidas en el mercado de ciberseguridad.
4.33	La solución debe de incluir varias técnicas de detección de virus, como basadas en coincidencia de patrones, Heurísticas y/o Emulación.
4.34	Incluir protección de brotes de virus a gran escala y de ataques no virales más pequeños, como estafas de phishing y distribución de malware, a medida que ocurren.
4.35	Incluir protección avanzada contra malware (amenazas) de día cero.
4.36	Incluir protección de amenazas basado en archivos adjunto en el correo electrónicos que permite entregar la reputación de archivos conocidos, análisis del comportamiento de ciertos archivos que aún no son conocidos por el servicio de reputación y evaluar continuamente las amenazas emergentes a medida que se dispone de nueva información y notificarle acerca de los archivos que se determina que son amenazas después de haber ingresado a su red.
4.37	Incluir herramientas que apoyen al operador a diagnostica y resolución de problema con el sistema de correo electrónicos.
4.38	La solución debe poder entregar servicios de análisis de archivos y reputación de archivos.
4.39	Capacidad de realizar lista negra (blackilist) y lista blanca (whitelist) en correo electrónicos.
4.40	Debe contar con una garantía directamente de fábrica de al menos de tres (3) años o treinta y seis (36) meses.
4.41	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
4.42	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
5	***SEGURIDAD WEB***
5.01	La solución debe proveer seguridad web para un total de 850 usuarios de la institución

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

5.02	La implementación de la solución debe soportar el proxy transparente, explicito e hibrido
5.03	La solución debe poder interceptar solicitudes sobre protocolo HTTP, HTTPS, FTP y SOCKS
5.04	Integración con los servidores de identidad de la institución, tales como Active Directory y LDAP
5.05	La autenticación de los usuarios finales debe ser de forma transparente sin intervenir el dispositivo o usuario final y consentimiento del usuario (Single-Sign-On)
5.06	Realizar Single Sign-On sin necesidad de instalar un agente en el dispositivo final.
5.07	Poder realizar inspección de trafico cifrado sobre protocolo HTTP (HTTPS)
5.08	La solución debe tener la capacidad de validar los certificados digitales, como Certificado no expirado, Entidad Certificadora Reconocida, Certificado no revocado, entre otros, antes de proceder con la inspección de trafico cifrado
5.09	Capacidad de agregar certificado de entidad certificadora local a la lista de entidades certificadores de confianza en la solución
5.10	Debe soporta política de control Web basado en protocolo y User Agents
5.11	Capacidad de agregar y controlar URL personalizadas en la solución de seguridad web
5.12	Contar con categoría de URL predefinidas
5.13	Poder obtener visibilidad y control de las aplicaciones
5.14	Capacidad de implementar controles de acceso de aplicaciones basado en la identidad del usuarios o red.
5.15	Capacidad de regular el consumo de ancho de banda
5.16	La solución debe poder almacenar datos en caché para aumentar el rendimiento
5.17	Debe permitir personalizar el almacenamiento en cache, como excluir URL específicas del almacenamiento en caché
5.18	La solución debe poder permitir bypass de seguridad Web
5.19	Poder realizar filtrado de contenido web basado en la reputación web del sitio
5.20	Capacidad de Safe Search y puntuación de contenido sitio (Site Content Rating) que identifique y garantice una navegación segura.

SECCION DE COMPRAS Y CONTRATACIONES
BAGRICOLA

5.21	Capacidad de entregar una visibilidad y control granular de las aplicaciones que permita: ▪ Controlar los comportamientos de la aplicación ▪ Controlar la cantidad de ancho de banda utilizado para tipos de aplicaciones particulares ▪ Notificar a los usuarios finales cuando estén bloqueados ▪ Asignar controles a aplicaciones de mensajería instantánea, blogs y redes sociales ▪ Especificar la configuración de Solicitud de rango
5.22	La solución debe entregar la detección y el bloqueo de malware, análisis continuo y alertas retrospectivas
5.23	Capacidades de detección y bloqueo de malware a través de la reputación de archivos, informes detallados del comportamiento de los archivos, análisis continuo de archivos y alertas de veredicto retrospectivo
5.24	Capacidad de escanear continuamente las actividades de la red que permita detectar y bloquear el malware que intenta eludir la solución de Seguridad Web.
5.25	La solución debe poder combinar el filtrado de URL tradicional con el análisis de contenido dinámico para mitigar los riesgos de cumplimiento, responsabilidad y productividad.
5.26	La base de datos de filtrado de URL debe continuamente ser actualizada.
5.27	La solución debe poder escanear el texto, califica el texto para determinar su relevancia, calcula la proximidad del documento del modelo y devolver la categoría más cercana basada en el contexto del sitio web.
5.28	La solución propuesta debe ser virtual bajo la plataforma de virtualización de Microsoft Hyper-V.
5.29	Contar con reportes predefinidos por el fabricante.
5.30	Permita crear o personalizar reporte de seguridad y red, de acuerdo con aplicaciones, malware, intrusión, etc.
5.31	Permitir descargar o exportar los reportes de seguridad generado en la solución.
5.32	Permitir enviar reportes de seguridad a un repositorio externo.
5.33	Permitir almacenar reportes de seguridad de forma local.
5.34	Entregar los reportes en formato de archivo de al menos PDF.
5.35	Capacidad de enviar alertas vía correo electrónico.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

5.36	Poder enviar alertas de acuerdo con la severidad del evento disparada por la solución, tales como crítico, advertencia, informativo, etc.
5.37	Autoridad de enviar alertas relacionada al sistema y hardware de la solución propuesta.
5.38	Enviar alertas de eventos de malware o archivos maliciosos.
5.39	Enviar alertas si algunos de servicios de seguridad de la solución propuesta pueden o presenta inconveniente en su correcto funcionamiento.
5.40	Capacidad de enviar alertas cuando el licenciamiento de la solución propuesta está próximo a expirar.
5.41	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
5.42	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
5.43	Permitir la creación de grupo de usuarios con diferentes niveles de privilegio.
5.44	Permitir la integración con Active Directoy (Usuarios y Grupo de usuarios).
5.45	Debe contener análisis real-time de trafico web para realizar troubleshooting.
6	***SEGURIDAD DE PUNTOS FINALES (ENDPOINTS)***
6.1	La solución debe tener la capacidad de brindar seguridad para un total de **870** Endpoint o puntos finales.
6.2	La solución de seguridad de puntos finales propuesta debe ser nativa en la nube.
6.3	Debe de contar con una administración centralizadas de todos los Endpoint o puntos finales licenciado.
6.4	Debe permitir tener acceso a la consola de administración centralizadas desde cualquier navegador o explorador, sin necesidad de un instalar ningún software adicional.
6.5	Debe asegurar Endpoint o puntos finales basados en Windows, MacOS, Linux.
6.6	Debe contar con multiplex capa de protección integrada para la seguridad de los puntos finales.
6.7	No debe de ser requerido más de un agente o conector en el punto final para lograr todas las funcionalidades seguridad para Endpoint o puntos finales.

6.8	Debe de permitir escalabilidad sin necesidad de agregar ningún hardware o componente, solo agregando más licencias.
6.9	Incluir funcionalidad de reputación de archivos que permita entregar la disposición (mala o buena) de archivos.
6.10	Proporcionar una base de datos completa de todos los archivos que se han visto y su correspondiente buena o mala disposición. Garantizando que el malware conocido se coloque en cuarentena rápida y fácilmente en el punto de entrada sin ningún escaneo intensivo del procesador.
6.11	Capacidad de sincronización y estabilidad de actualización permanente con motores de ciberseguridad ante amenazas y variantes.
6.12	Consumo bajo o moderado de memoria y performance CPU en los computadores y servidores.
6.13	Incluir motores antivirus basados en definiciones que se actualicen constantemente en los puntos finales de Windows, Mac o Linux.
6.14	Capacidad de detectar y prevenir malware polimórficos mediante similitudes entre el contenido del archivo sospechoso y el contenido de familias de malware conocidas, y condenar si hay una coincidencia sustancial.
6.15	Capacidad para "aprender" a identificar archivos y actividades maliciosos en función de los atributos del malware conocido.
6.16	Incluir prevención de exploits para aplicaciones vulnerables, procesos del sistema operativo o ataque de inyección de memoria basados en exploits
6.17	Proveer funcionalidad de protección de scripts.
6.18	Incluir funcionalidad de protección basado en comportamiento a través del monitoreo continuo de toda la actividad del usuario y del Endpoint que permite identificar y bloquear el comportamiento malicioso en tiempo real.
6.19	Capacidad para monitorear continuamente toda la actividad de los Endpoint y proporcionar detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el Endpoint.
6.20	Permitir escribir indicadores de compromisos (IoC) personalizados en un formato estándar abierto (OpenIOC).
6.21	Capacidad de identificar software vulnerable en los Endpoint, como también enumerar y priorizar en función de la puntuación CVE (Common Vulnerabilities and Exposures) de la industria.

SECCION DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

6.22	Capacidad de identificar automáticamente los ejecutables que existen en cantidades reducidas en los Endpoint y analizar esas muestras en entorno de pruebas (sandboxing) para descubrir nuevas amenazas.
6.23	Entregar un panel de informaciones o reporte que incluya eventos, puntos finales comprometidos, puntos finales que requieren atención inmediata, tipos de compromisos, entre otros.
6.24	Incluir funcionalidad de análisis forense que permita mostrar el alcance completo de unas amenazas en los puntos finales, tales como aplicaciones, procesos, punto de entrada, método, entre otros.
6.25	Incluir sandboxing de forma integrada.
6.26	Capacidad de análisis retrospectivo a través del monitoreo continuo y correlación de eventos de amenazas de seguridad que permita retroceder en el tiempo y automáticamente poner en cuarentena los archivos que en el momento comiencen a mostrar un comportamiento malicioso.
6.27	Proveer visibilidad de la línea de comando que permita determinar si las aplicaciones legítimas, incluidas las utilidades de Windows, se utilizan con fines maliciosos. Tales como explotaciones basadas en PowerShell, escalada de privilegios; modificaciones de listas de control de acceso e intento de enumeración del sistema.
6.28	Capacidad de aislar los Endpoint que se han visto comprometidos para detener la propagación de las amenazas y evitar que se comuniquen con sus C&C.
6.29	Permitir búsqueda avanzadas del malware en los puntos finales.
6.30	Incluir análisis retrospectivo de forma automática para detectar, alertar, rastrear, analizar y corregir retrospectivamente el malware avanzado que al principio puede parecer limpio o que evade las defensas iniciales y luego se identifica como malicioso.
6.31	Capacidad para mostrar una visualización clara y concisa de las interacciones del dispositivo final con malware, archivos, dominios y direcciones de red que facilite la investigación de incidentes y la contención rápida de amenazas.
6.32	Capacidad de integración con sandboxing en la premisa.
6.33	Soporte de API para extraer eventos, indicadores de compromiso (IoC) y datos del dispositivo.
6.34	Capacidad de aislar los puntos finales con eventos de compromisos u comprometido por malware de forma automática.
6.35	Entregar visibilidad del alcance de una infracción (cuántos Endpoint se ven afectados por el malware en cuestión). Descubrir al paciente cero: cuándo se vio por primera vez el malware, en qué computadora de

	la institución, cuál es su parentesco y cómo se mueve entre los dispositivos finales y las conexiones a las direcciones IP / dominio que establece.
6.36	Capacidad de lista blanca y lista negra que permitan sobrescribir la disposición entregada por la solución.
6.37	Contar con al menos 200 consultas predefinidas que permitan ejecutar consultas en vivo y programadas en todos los puntos finales utilizando una tecnología basada en osquery.
6.38	Capacidad de remover o poner en cuarentena de forma automática un archivo malicioso
6.39	Entregar causa raíz de la infección del malware en la cual se pueda observar las aplicaciones que intentando introducir malware a la institución.
6.40	Permitir realizar búsqueda de cualquier archivo cuestionable, ver la dispersión a través de una base instalada y extraer el archivo de cualquier Endpoint para su análisis y análisis forenses adicionales.
6.41	Debe mantener la protección fuera de línea con al menos funcionalidades de seguridad de prevención de exploits y antivirus.
6.42	Capacidad de permitir realizar análisis de archivos en específicos, que permita detallar el análisis de metadato, indicadores de comportamiento, tráficos de red, procesos, actividades de procesos, entre otros.
6.43	Incluir capacidad de EDR (Endpoint Detection and Response, por su sigla en inglés).
6.44	Contar con reportes predefinidos.
6.45	Capacidad de enviar reportes de seguridad de los Endpoint vía correo electrónicos.
6.46	Permitir crear, personalizar y eliminar reportes por el operador de la solución propuesta.
6.47	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
6.48	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
6.49	La solución debe permitir ver mediante análisis los datos del usuario, incluyendo User Name y Workstation.
6.50	Permitir la asignación de privilegios a usuarios administrativos de la solución propuesta.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

7	SEGURIDAD DE DNS RECURSIVO
7.1	La solución deberá brindar seguridad en la capa DNS recursivos a un total de 850 usuarios.
7.2	La solución deber ser un servicio de seguridad en la nube integrado en la base de Internet.
7.3	Capacidad de hacer cumplir la seguridad en las capas de DNS e IP, bloquear solicitudes de malware, ransomware, phishing y botnets incluso antes de que se establezca una conexión.
7.4	Detención de las amenazas en cualquier puerto o protocolo antes de que lleguen a la red o puntos finales.
7.5	Bloquear malware sin latencia en la red de la institución y/o puntos finales.
7.6	Proporcionar visibilidad de los servicios en la nube autorizados y no autorizados que se utilizan en toda la empresa, para que pueda descubrir nuevos servicios que se utilizan, ver quién los está utilizando, identificar el riesgo potencial y bloquear aplicaciones específicas fácilmente.
7.7	Como servicio entregado en la nube, debe proporcionar la visibilidad necesaria para proteger el acceso a Internet en todos los dispositivos de red, ubicaciones de oficinas y usuarios remotos/roaming.
7.8	Protección a usuarios remotos/roaming, aunque no estén conectados a la red por medio de VPN o protección en ausencia de la VPN.
7.9	Agente o cliente para usuarios remotos/roaming soportando Windows OS y Mac OSX.
7.10	Provee máquinas virtuales para el reconocimiento de las IP Privadas realizando NAT e integración con Active Directory.
7.11	Proteger cualquier dispositivo en la red corporativa
7.12	Evita Malware, ataques phishing, Command & Control Callback a través de cualquier puerto.
7.13	Bloquea Minado de Crypto-Monedas y dominios nuevos.
7.14	Detiene uso de violaciones aceptable de uso (más de 80 categorías) y refuerzo a SafeSearch.
7.15	Realizar filtrado web basado en dominio o categoría de dominios.
7.16	Permitir crear lista negras y blancas basada en dominio.
7.17	Crear políticas y ver informes por red (IP de salida),subred interna, dispositivo de red, dispositivo de roaming/moviles y grupo de Active Directory (incluidos usuarios específicos).
7.18	Los registro de logs para los dominios debe ser de 30 días (detalles) y un (1) año histórico.
7.19	Retención de Logs en Amazon Web Services.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

7.20	Incluir API para reportes
7.21	Descubrimiento y bloqueo de aplicaciones para combatir Shadow IT
7.22	Identificación de ataques locales vs ataques globales/ trafico DNS global
7.23	Bloqueo personalizable y granular de páginas y opciones de omisión
7.24	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
7.25	Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
8	***SEGURIDAD DE DOBLE FACTOR DE AUTENTICACIÓN***
8.1	La solución deber ser SaaS.
8. 2	Debe soportar un mínimo de 200 usuarios finales.
8.3	Proporcionar una aplicación de autenticación móvil segura.
8.4	Proveer aprobación rápida y basada en notificaciones push para verificar la identidad de su usuario con soporte para teléfonos inteligentes, relojes inteligentes y tokens U2F.
8.5	Permitir una variedad de otros métodos de autenticación compatibles para satisfacer las necesidades de cada usuario.
8.6	Debe soportar los siguientes métodos de doble factor de autenticación: Push, U2F USB, Biometrico, Token y Passcodes.
8.7	Permitir diferentes opciones de aprovisionamiento de usuarios en la solución propuesta, tales como: sincronización de directorio avanzado, inscripción masiva y auto inscripción de usuarios.
8.8	Capacidad de utilizar API de administración en la solución que nos permita interactuar con los registros de seguridad de la solución para fines de informes y análisis personalizados.
8.9	Entregar un resumen de alto nivel del estado de seguridad de los dispositivos (endpoint) que cada vez que acceden a las aplicaciones.
8.10	Capacidad de limitar el acceso a las aplicaciones en función de las necesidades de seguridad.
8.11	Capacidad de administrar los permisos por grupo de usuarios y dispositivos de confianza.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

8.12	Soportar SSO (Single-Sign On) seguro basado en la nube.
8.13	Poseer la capacidad de simplificar la configuración de SSO con integraciones listas para usar con aplicaciones en la nube y establecer políticas granulares para cada aplicación en la nube basadas en el riesgo que permita mejorar la seguridad del acceso.
8.14	Soportar integración con aplicaciones locales, basadas en la web y basadas en la nube para doble factor de autenticación.
8.15	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
8.16	Soportar integración con servidor de Microsoft Active Directory, como servidor de identidad.
9	***INTEGRACIÓN DE ARQUITECTURA DE CIBERSEGURIDAD***
9.1	Las soluciones debe de contar con la capacidad de funcionar con productos de terceros a través de API.
9.2	Las soluciones de los ITEMS deben integrarse de forma nativa.
9.3	La integración entre las soluciones debe permitir desde una única consola de interfaz gráfica la de realizar repuestas amenazas (Threat Response).
9.4	Incluir orquestación con flujos de trabajo prediseñados alineados con casos de uso comunes y un lienzo de arrastrar y soltar sin código o con poco código para crear flujos propios de trabajo para eliminar la fricción en procesos y automatización de las tareas de rutina de respuesta a incidentes o amenazas.
9.5	Entregar panel que ofrezca una vista de la infraestructura de seguridad para una visibilidad unificada e inteligencia agregada y procesable en todo el entorno de seguridad de la empresa.
9.6	Las soluciones de seguridad deben permitirnos la flexibilidad de crecer por los menos un 19% en la totalidad de las licencias solicitada de cada tipo, sin que esto incurra en costo o facturación adicional para la institución.
10	***Solución de Security Information and Event Management (SIEM)***
10.1	La solución propuesta debe estar implementada en la premisa de la institución de forma física (hardware).
10.2	Incluir un total de 75 agentes.
10.3	Incluir un total de 100 dispositivos (servidores y equipos de redes).

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

10.4	Capacidad de almacenamiento mínima: 6 TB (La capacidad neta utilizable debe garantizar mínimo un año de retención).
10.5	Capacidad de Memoria RAM mínima: 24 GB o Superior.
10.6	Procesador de gran capacidad. Ejemplo: Intel Xeon E5-2620V3 6C12T 2.40 GHz
10.7	Fuente de poder redundante.
10.8	Capacidad mínima de procesamiento de 1000 eventos por segundo.
10.9	Contracto de soporte a 36 meses por fábrica en el hardaware.
10.10	Aprendizaje automático / UEBA.
10.11	Puntuación de riesgo de usuario y dispositivo.
10.12	Correlación de eventos distribuidos en tiempo real.
10.13	Descubrimiento automatizado de infraestructura en tiempo real y Application Discovery Engine (CMDB).
10.14	Asignación dinámica de identidad de usuario
10.15	Administración de correlación de eventos agrupados como servicio
10.16	Infusión de inteligencia de seguridad (Threat Intelligence)
10.17	Informes de cumplimiento listos para usar y exportables
10.18	Monitoreo de cambios de configuración en tiempo real
10.19	Supervisión del rendimiento mediante panel de monitoreo
10.20	Monitoreo de disponibilidad
10.21	Analítica potente y escalable
10.22	Notificación y Sistema de gestión de incidentes Integrados
10.23	Los VA debe proporcionarse para: VMWare, Hyper-V, KVM iv, Imagen de AWS disponible y Azure.
10.24	El SIEM Clúster puede escalar agregando VA adicional al clúster. Esta capacidad de escalamiento debe: - Proporcione correlación de reglas distribuidas en tiempo real en memoria en todos los componentes del clúster. - Proporcione reportes distribuidos y reportes analíticos a través del Clúster SIEM. Esto debe ser

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

	automático y el usuario no debería necesitar especificar qué componente necesita ejecutar una búsqueda En el sistema de gestión central de SIEM.
10.25	El Clúster de SIEM no debe limitar la cantidad de datos de eventos que se almacenan. Este límite solo debería ser la cantidad de almacenamiento que se proporciona.
10.26	El SIEM Clúster debería ser capaz de escalar, esto significa que el SIEM Clúster puede comenzar con un solo VA y escalar agregando más VA. Los datos de eventos se pueden almacenar en un disco virtual cuando se trabaja con un solo VA y también en NFS cuando se trabaja con el SIEM Clúster (VA múltiples). Nota: no debe existir ningún licenciamiento adicional para el despliegue nuevos VA.
10.27	El SIEM Clúster debe poder escalar a más de 500K EPS
10.28	El SIEM Clúster debe poder almacenar tanto el registro de eventos brutos como el registro de eventos analizados / datos normalizados.
10.29	No debería haber ningún requisito para un nivel de "almacenamiento" separado que filtre o envíe un subconjunto de eventos reenviados por los recopiladores a un nivel de correlación. El SIEM Clúster debe poder procesar cada evento reenviado por el nivel de colección.
10.30	Los datos del evento deben almacenarse en un modo comprimido.
10.31	El SIEM Clúster no debe usar una base de datos relacional (MS SQL, Postgresql, MySQL, Oracle) para almacenar los datos del evento. Se debe usar una base de datos moderna para almacenar datos de eventos como una base de datos no SQL.
10.32	Una base de datos relacional se puede usar para almacenar plantillas, incidentes y otra información estructurada.
10.33	Él VA debe ejecutarse en Linux y tener la capacidad de actualizar los paquetes del sistema operativo.
10.34	El SIEM debe ser capaz de recopilar contexto adicional más allá de los datos de registro de los dispositivos y esto debe lograrse mediante el descubrimiento activamente de los dispositivos dentro de la red sin un agente y usar protocolos estándar tales como: SNMP, WMI, VM SDK, OPSEC, JDBC, Telnet, SSH, JMX
10.35	Capacidad para controlar el estado y la capacidad de respuesta de los servicios, incluidos DNS, FTP / SCP, TCP / UDP genérico, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH y Web - HTTP, HTTPS (paso único y paso múltiple).

10.36	Los resultados de este monitor de disponibilidad se pueden usar para calcular la capacidad del servicio, como la disponibilidad de un servicio que está disponible al 99%.
10.37	Una vez descubierta, la inmersión debe presentarse en una Base de Datos de Gestión de Configuración (CMDB) dentro de la solución SIEM y mostrarse como mínimo, Versión / Firmware / OS instalado en el dispositivo.
10.38	Número de serie del dispositivo, Interfaces configuradas en el dispositivo junto con: Nombre de la interfaz, IP y subred, Estado de la interfaz (habilitado, deshabilitado), Cualquier nivel de seguridad configurado en el dispositivo, La velocidad de la interfaz, La velocidad y el nombre de la interfaz deben ser editables, Procesos que se ejecutan en el dispositivo o sistema operativo.
10.39	Alertar cuando hay un cambio en el estado del proceso al monitorear activamente usando protocolos como se describe en los protocolos 3.a. Por ejemplo, alerta cuando un proceso o servicio se detiene.
10.40	Los dispositivos se deben llenar automáticamente dentro de Grupos en la CMDB, por ejemplo, Grupo de servidores de Windows, Grupo de cortafuegos.
10.41	Las aplicaciones que se ejecutan en dispositivos deben descubrirse automáticamente y la CMDB debe tener un grupo de aplicaciones que llene automáticamente los dispositivos del grupo. Por ejemplo, el grupo de aplicaciones ""Servidores IIS"" debe enumerar todos los dispositivos que ejecutan Microsoft IIS.
10.42	Ser capaz de informar sobre toda la información dentro de la CMDB: - Informe sobre el firmware de los dispositivos o el número de versión - Proporcione un informe de auditoría con aprobación / falla, ya sea que el dispositivo tenga la versión apropiada de Versión / Firmware / SO instalada en el dispositivo.
10.43	Una vez que se complete el descubrimiento activo de los dispositivos, el SIEM debe tener una plantilla incorporada que definirá automáticamente qué métricas se recopilarán para los dispositivos y los intervalos de recolección.
10.44	Las métricas de rendimiento recopiladas deben incluir: Uso de la interfaz, errores, bytes enviados y recibidos, UPC, Memoria, Disco, Utilización del proceso.
10.45	Debe tener la capacidad de monitorear la capacidad de almacenamiento de la plataforma Netapp.
10.46	Debe soportar el monitoreo de la infraestructura de Telefonia IP a través de IPSLA.
10.47	Debe soportar el uso de Netflow, Sflow, y Cisco AVC.
10.48	El SIEM debería ser capaz de descubrir Active Directory y LDAP y mostrar el directorio en la GUI.
10.49	Capacidad de recopilar eventos de Windows a través de WMI y agente.

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

10.50	El SIEM debe proporcionar una interfaz de análisis unificada que permita que el mismo lenguaje de consulta analice tanto los datos de registro como los datos de rendimiento.
10.51	El sistema debería poder incluir eventos en los recopiladores que no son relevantes o que no son necesarios. Esto no debería afectar ninguna licencia.
10.52	Tanto los datos brutos, analizados y enriquecidos se deben pasar al clúster SIEM desde los recopiladores.
10.53	El procesamiento de datos de eventos debe ser realizado por analizadores sintácticos en el sistema.
10.54	Todos los analizadores deberían poder ser modificados y personalizados.
10.55	Los analizadores personalizados deberían poder crearse y definirse en la GUI sin acceso CLI.
10.56	Se pueden agregar nuevos atributos (variables analizadas), dispositivos y tipos de eventos a través de la GUI sin acceso CLI.
10.57	Los dispositivos se pueden monitorear sin agentes a través de SSH, telnet WMI, JMX y PowerShell.
10.58	El SIEM debe proporcionar acceso basado en roles para restringir el acceso a los datos y también restringir el acceso a la GUI.
10.59	El directorio se puede usar en condiciones de filtro dentro de informes y análisis.
10.60	Los analizadores deben definirse en un marco XML con las siguientes capacidades: a. Capacidad de definir patrones que se repiten como variables. b. Posibilidad de definir funciones para identificar pares clave de valores c. Capacidad para realizar pruebas y funciones de casos d. Capacidad de realizar transformaciones en los datos en la etapa de análisis sintáctico.
10.61	El SIEM debe tener la capacidad de proporcionar un Agente de Windows que tenga las siguientes capacidades: a. Agentes administrados centralmente b. Capaz de recoger registros de archivos de texto en dispositivos con Windows c. Capaz de recopilar registros de eventos que no sean Seguridad, Sistema y Aplicación d. Realizar la supervisión de integridad de archivos e. Realizar el seguimiento del registro f. Monitor para dispositivos extraíbles g. Ejecute los comandos de PowerShell y envíe de vuelta la salida como registros h. Ejecutar comandos WMI y enviar de vuelta la salida como registros i. El agente de Windows debe enviar datos de eventos a los componentes de SIEM cifrados mediante HTTPS

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

10.62	Los métodos de autenticación externa deben ser compatibles e incluyen: a. Directorio Activo b. LDAP c. RADIUS
104.63	Posibilidad de integrar feeds de Threat Intelligence (TI).
10.64	Cada TI ((Threat Intelligence) puede admitir hasta 200.000 entradas
10.65	Se deben proporcionar varias integraciones a TI comerciales y del fabricante de la solución de SIEM.
10.66	Se debe proporcionar una cantidad de integraciones a Open Source TI en la caja.
10.67	Posibilidad de correlacionar datos de TI en tiempo real, en memoria contra datos de eventos.
10.68	Posibilidad de correlacionar datos de TI con datos de eventos históricos.
10.69	Capacidad de consultar eventos en una vista analítica en un modo de transmisión, de modo que se informe sobre eventos antes de almacenarlos en el disco.
10.70	Proporcione informes listos para usar, sin costo adicional, para: a. PCI-DSS b. HIPAA c. SOX d. NERC e. FISMA f. ISO g. GLBA h. GPG13 i. Controles críticos SANS
10.71	Capacidad para exportar e importar paneles, informes y reglas a través de XML
10.72	Posibilidad de reenviar cualquier información de evento recopilada a través de KAFKA.
10.73	Capacidad para recopilar la configuración del dispositivo de red, identificar cambios y proporcionar una comparación lado a lado.
104.74	Monitoreo del sistema arriba / abajo - a través de Ping, SNMP, WMI, Uptime, Análisis e interfaz crítica.
10.75	Proceso crítico y servicio, BGP / OSPF / EIGRP, cambio de estado y estado de puerto arriba / abajo.

SECCION DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

10.76	Modelado de disponibilidad del servicio a través del monitoreo de transacciones sintéticas- Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP /UDP.
10.77	Las visualizaciones del tablero deben admitir tipos de gráfico de: a. Bar b. Tarta c. Línea d. Mesa e. Combinación (línea y vista de tabla) f. Treemap g. Gráfico de dispersión h. Valores individuales i. Calibradores j. Mapa Geográfico
10.78	Marco de notificación de incidentes basado en políticas.
10.79	Posibilidad de activar un script de corrección cuando ocurre un incidente especificado.
10.80	La integridad de los datos del evento se puede verificar a través de la GUI recalculando el hash de los datos del evento con un hash almacenado dentro del SIEM en el momento de escribir los eventos en el disco.
10.81	Integración basada en API a sistemas de tickets externos: ServiceNow, ConnectWise y Remedy.
10.82	Posibilidad de ampliar la integración del sistema de tickets a través de API.
10.83	Sistema integrado de emisión de boletos o Tickets.
10.84	Activar patrones de eventos complejos en tiempo real.
10.85	Explorador de incidentes: vinculación dinámica de incidentes con hosts, IP y usuario para comprender todos los incidentes relacionados rápidamente Cuadros de mandos personalizables ricos.
10.86	Tableros configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar los KPI.
10.87	Informes y análisis compartibles entre organizaciones y usuarios.
10.88	Codificado por colores para identificar rápidamente problemas críticos.
10.89	Busque eventos en tiempo real, sin la necesidad de indexar y usar operadores lógicos como AND, OR, NOT y paréntesis.

SECCION DE COMPRAS Y CONTRATACIONES
BAGRICOLA

10.90	Búsquedas basadas en palabras clave y búsquedas por atributos de eventos analizados contra datos.
10.91	Buscar eventos históricos: consultas similares a SQL con condiciones de filtro booleanas, grupos por agregaciones relevantes, filtros de hora del día, coincidencias de expresiones regulares, expresiones calculadas, GUI y API.
10.92	Patrones completos que admiten la lógica booleana completa y permiten: - Sub patrones conectados en la dimensión de tiempo por operadores como AND, OR, FOLLOWED BY, AND NOT, y NOT FOLLOWED_BY, - Cada sub patrón puede filtrar y aplicar operadores de agregación como AVG, MAX, MIN, COUNT y COUNT DISTINCT, - Los umbrales pueden ser estáticos o estadísticamente derivados de datos pro.
10.93	El perfil estadístico y las alertas de eventos deberían incluir - Promedios móviles - Desviaciones estándar
10.94	Recopilar archivos de configuración de red, almacenados en una versión repositorio.
10.95	Recopilar versiones de software instaladas, almacenadas en una versión repositorio.
10.96	Detección automatizada de cambios en la configuración de red y software instalado.
10.97	Detección automática de cambios de archivo / carpeta - Windows y Linux.
10.98	Detección automatizada de cambios de un aprobado archivo de configuración.
10.99	Detección automática de cambios en el registro de Windows a través de agente de Windows.
10.100	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
	SEGURIDAD PERIMETRAL Y CONECTIVIDAD OFICINA REMOTAS
11	***Solución de NGFW para Conectividad VPN en Oficina Principal***
11.1	La solución debe entregar un rendimiento de Firewall de 27 Gbps, IPS 5 Gbps, NGFW 3.5 Gbps y Threat Protection 3 Gbps.
11. 2	La solución debe soportar 3 millones de sesiones concurrentes (TCP)
11. 3	La solución debe soportar Nuevas sesiones / segundo (TCP) 280.000
11.4	La solución debe soportar sin necesidad de licenciamiento al menos 2,500 túneles VPN IPsec puerta a puerta.

11.5	La solución debe soportar sin necesidad de licenciamiento al menos 16,000 túneles VPN IPsec de cliente a puerta de enlace.
11.6	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
11.7	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
11.8	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
11.09	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
11.10	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding.
11.11	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
11.12	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
11.13	Tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios.
11.14	Implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
11.15	La solución debe soportar VPN de sitio-a-sitio y cliente-a-sitio.
11.16	La solución debe soportar VPN IPSec.
11.17	La solución debe soportar VPN SSL.
11.18	La VPN IPSec debe ser compatible con 3DES.
11.19	La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-4.
11.20	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
11.21	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
11.22	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
11.23	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI.
11.24	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.

11.25	La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.
11.26	Las características de VPN SSL se deben cumplir con o sin el uso de agentes.
11.27	La solución debe soportar la asignación de DNS en la VPN de cliente remoto.
11.28	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
11.29	La solución debe soportar la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
11.30	La solución debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
11.31	La solución debe incluir 1x USB Port .
11.32	La solución debe incluir 1x Console Port.
11.33	La solución debe incluir 2x GE RJ45 MGMT/DMZ Ports .
11.34	La solución debe incluir 2x GE RJ45 WAN Ports .
11.35	La solución debe incluir 2x GE RJ45 HA Ports
11.36	La solución debe incluir 14x GE RJ45 Ports SOC3 1U RPS / 480GB 7. 2x GE RJ45/SFP Shared Media Pairs
11.37	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses mínimo en piezas y funcionalidad de seguridad con un SLA mínimo de 24X7, lo cual garantice el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento. Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
11.38	La solución debe de ser factor forma Rack Mount, 1 RU.
11.39	Debe incluir licencia de IPS.
11.40	Debe incluir licencia de protección avanzada contra virus.
11.41	Debe incluir licencia de control de aplicaciones.
11.42	Debe incluir licencia de filtrado web y video.
11.43	Debe incluir licencia anti-spam.

11.44	La solución debe de estar en alta disponibilidad.
11.45	Debe incluir 4 módulos a 10GB SFP+, como también los cables de fibras de 5M a 10M.
11.46	Incluir al menos cuatros (4) cables de cobres de 5M a 10M.
12	***Solución de NGFW para Conectividad VPN en Oficina Remotas***
12.1	La solución debe entregar un rendimiento de Firewall 5 Gbps, IPS 1 Gbps, NGFW 800 Mbps y Threat Protection 600 Mbps.
12.2	La solución debe soportar 700 mil sesiones concurrentes (TCP).
12.3	La solución debe soportar Nuevas sesiones / segundo (TCP) 35.000.
12.4	La solución debe soportar sin necesidad de licenciamiento al menos 200 túneles VPN IPsec puerta a puerta.
12.5	La solución debe soportar sin necesidad de licenciamiento al menos 250 túneles VPN IPsec de cliente a puerta de enlace.
12.6	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
12.7	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
12.8	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
12.9	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
12.10	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding.
12.11	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
12.12	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
12.13	Tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios.
12.14	Implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
12.15	La solución debe soportar VPN de sitio-a-sitio y cliente-a-sitio.
12.16	La solución debe soportar VPN IPSec.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

12.17	La solución debe soportar VPN SSL.
12.18	La VPN IPSec debe ser compatible con 3DES.
12.19	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA256, SHA384 y SHA512.
12.20	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14 hasta Grupo 32.
12.21	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
12.22	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
12.23	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI.
12.24	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
12.25	La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.
12.26	Las características de VPN SSL se deben cumplir con o sin el uso de agentes.
12.27	La solución debe soportar la asignación de DNS en la VPN de cliente remoto.
12.28	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
12.29	La solución debe soportar la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
12.30	La solución debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
12.31	La solución debe incluir 1x USB Port .
12.32	La solución debe incluir 1x Console Port.
12.33	La solución debe incluir 1x GE RJ45 WAN.
12.34	La solución debe incluir 3x GE Ethernet Ports.
12.35	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
12.36	Debe incluir licencia de IPS.

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

12.37	Debe incluir licencia de protección avanzada contra virus.
12.38	Debe incluir licencia de control de aplicaciones.
12.39	Debe incluir licencia de filtrado web y video.
12.40	Debe incluir licencia anti-spam.
12.41	La solución debe cubrir un total de 63 oficinas remotas.
12.42	Incluir al menos (2) cables de cobres de 5M a 10M por cada oficina remota.
13	***Gestión Centralizadas de los NGFW***
13.1	La solución debe ser virtual y compatible con el ambiente Vmware, Microsoft Hyper-V, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM on Redhat 6.5+ y Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) y Alibaba Coud (AliCloud).
13.2	La solución no debe haber límites a la cantidad de múltiples vCPU.
13.3	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.
13.4	Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
13.5	Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
13.06	Soporte SNMP versión 2 y 3.
13.07	Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
13.08	Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
13.09	Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH, API abierta.
13.10	Soportar autenticación de usuarios de acceso a la plataforma vía LOCAL, LDAP, Radius y TACACS+
13.11	Debe tener capacidades de Alta disponibilidad (HA).
13.12	Debe tener la capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.

13.13	Como parte de la visibilidad SD-WAN de los dispositivos gestionados centralmente, la solución debe contar con visibilidad de estado de enlace, desempeño de aplicación, utilización de ancho de banda y cumplimiento de SLA objetivo.
13.14	Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola.
13.15	La solución debe tener la capacidad Multi-tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue zerotouch para un aprovisionamiento masivo rápido.
13.16	La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos , conteniendo updates de todos los dispositivos gestionados.
13.17	Debe tener la capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.
13.18	La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
13.19	Permitir integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .
13.20	En la fecha de la propuesta, ninguno de los modelos de la oferta pueden estar en el sitio del fabricante en listados de end-of-life o end-of-sales.
13.21	Debe permitir acceso concurrentes de administradores.
13.22	Debe tener interfaz basada en línea de comando para administración de la solución de gestión.
13.23	Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
13.24	Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores.
13.25	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones.
13.26	Generar alertas automáticos por Email.
13.27	Generar alertas automáticos por SNMP.
13.28	Generar alertas automáticos por Syslog.
13.29	Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.

13.30	Debe ser permitido al administrador transferir los backups a un servidor FTP, SCP y SFTP.
13.31	Los cambios realizados en un servidor de gestión debe ser automáticamente replicados al servidor redundante.
13.32	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI).
13.33	Debe soportar sincronización de reloj interno por protocolo NTP.
13.34	Debe registrar las acciones efectuadas por cualquier usuario.
13.35	Deben proveerse manuales de instalación, configuración y operación de toda la solución, en los idiomas español, portugués o inglés, con presentación de buena calidad.
13.36	Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión.
13.37	Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API).
13.38	Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
13.39	La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización.
13.40	La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación.
13.41	La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware.
13.42	Funcionalidades de Gestión de Firewalls.
13.43	La gestión debe permitir la creación y administración de políticas de Filtro de URL.
13.44	Permitir buscar cuáles reglas un objeto está siendo utilizado.
13.45	Permitir la creación de reglas que permanezcan activas en horario definido.
13.46	La solución debe permitir ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados.
13.47	Debe tener capacidad de desplegar los resultados de auditoría de seguridad d elos dispositivos gestionados.
13.48	Permitir backup de las configuraciones y rollback de configuración para la última configuración salva.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

13.49	Debe tener mecanismos de validación de políticas avisando cuando hayan reglas que ofusquen o conflictúen con otras (shadowing).
13.50	Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas.
13.51	Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión.
13.52	La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta.
13.53	La solución debe permitir la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos.
13.54	Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados.
13.55	Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador.
13.56	Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos.
13.57	Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
13.58	Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware.
13.59	Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos.
13.60	Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración.
13.61	Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos.
13.62	Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión.

13.63	Permitir configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada.
13.64	Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos.
13.65	Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada.
13.66	Permitir la creación de reglas anti DoS de forma centralizada.
13.67	Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada.
13.68	Debe permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía.
13.69	Debe permitir el uso de DDNS en VPNs de manera centralizada.
13.70	Debe permitir la gestión de Access Points propietarios de manera centralizada.
13.71	Debe permitir la gestión de Switches propietarios de manera centralizada.
13.72	Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada.
13.73	La licencia debe soportar al menos 100 dispositivos o dominio virtuales para su administración centralizadas.
13.74	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
13.75	Incluir servicio de mejores prácticas directo de fábrica.
14	***Gestión y Almacenamiento de Logs de los NGFW***
14.1	La solución debe ser virtualizada y compatible con el ambiente Vmware, Microsoft Hyper-V, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM on Redhat 6.5+ y Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) y Alibaba Coud (AliCloud).
14.2	La solución no debe haber límites a la cantidad de múltiples vCPU.
14.3	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

14.4	Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
14.5	Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
14.6	Soporte SNMP versión 2 y 3.
14.7	Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
14.8	Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
14.9	Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.
14.10	Soportar autenticación de usuarios de acceso a la plataforma vía LDAP, Radius y TACACS+
14.11	Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos, burbuja y tabla.
14.12	Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
14.13	Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
14.14	Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.
14.15	Contar con mecanismos de borrado automático de logs antiguos.
14.16	Permitir la importación y exportación de reportes.
14.17	Debe contar con la capacidad de crear informes en formato HTML, PDF, XML y CSV.
14.18	Debe permitir exportar los logs en formato CSV.
14.19	Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
14.20	Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

14.21	La solución debe contar con reportes predefinidos.
14.22	Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.
14.23	Debe ser posible la duplicación de reportes existentes para su posterior edición.
14.24	Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
14.25	Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
14.26	Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
14.27	Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.
14.28	Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
14.29	Debe permitir descargar de la plataforma los archivos de logs para uso externo.
14.30	Tener la capacidad de generar y enviar reportes periódicos automáticamente.
14.31	Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
14.32	Permitir el envío por email de manera automática de reportes.
14.33	Debe permitir que el reporte a enviar por email sea al destinatario específico.
14.34	Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
14.35	Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
14.36	Debe permitir el uso de filtros en los reportes.
14.37	Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
14.38	Permitir especificar el idioma de los reportes creados.
14.39	Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
14.40	Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.

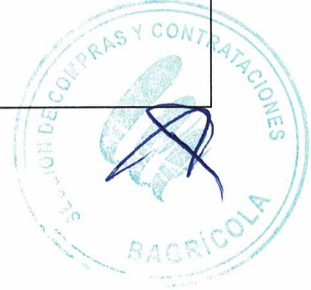
14.41	Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
14.42	Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
14.43	Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
14.44	Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
14.45	Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
14.46	Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
14.47	Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
14.48	Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos.
14.49	Debe permitir visualizar en tiempo real los logs recibidos.
14.50	Debe permitir el reenvío de logs en formato syslog.
14.51	Debe permitir el reenvío de logs en formato CEF (Common Event Format).
14.52	Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red.
14.53	Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
14.54	Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
14.55	Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red.
14.56	Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
14.57	Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.

14.58	Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
14.59	Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs..
14.60	Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).
14.61	Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC .
14.62	Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3..
14.63	Debe permitir generar alertas de eventos a partir de logs recibidos.
14.64	Debe permitir crear incidentes a partir de alertas de eventos para endpoint.
14.65	Debe permitir la integración al sistema de tickets ServiceNow.
14.66	Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
14.67	Debe permitir respaldar logs en nube publica de Amazon S3, Microsoft Azure y Google Cloud.
14.68	Debe soportar el estándar SAML para autenticación de usuarios administradores.
14.69	Debe contar con reporte de cumplimiento de PCI DSS..
14.70	Debe contar con reporte de utilización de aplicaciones SaaS.
14.71	Debe contar con reporte de prevención de perdida de datos (DLP).
14.72	Debe contar con reporte de VPN.
14.73	La licencia debe incluir 50 GB de log diario.
14.74	La solución ofertada debe contar con una garantía directa del fabricante por 36 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
14.75	Incluir licencia de indicadores de compromiso, SoC e inteligencia de seguridad directo de fábrica.
14.76	Debe soportar al menos 100 dispositivos para almacenamiento y gestión centralizada de logs.
	EQUIPOS DE RED PARA OFICINA PRINCIPAL Y REMOTAS
15	***SWITCH* DE CORE *DE OFICINA PRINCIPAL***

15.1	**Dos (02) Switch de Core Oficina Principal**
15.2	Administrable: Administrable vía CLI y vía una Plataforma de red Administrable por Software SDN. Requiere incluir las licencias para ser administrado de ambas manera.
15.3	24 puertos Velocidad 1/10G/25G 16 Ports Gigabit Ethernet compatibles con 1G, 10G, y 40G.
15.4	Uplink modular Velocidad 4x 40/100G 4Puertos.
15.5	Debe contar con cinco fan field-replaceable de velocidad variable y reemplazable en caliente, el mismo puede admitir la falla de uno de los fan sin que esto afecte su funcionamiento.
15.6	El flujo de aire debe ser front-to-back.
15.7	Incluir Power Supply Redundante AC 650W.
15.8	Soporte mínimo de 26,000 Security ACL.
15.9	Debe ocupar no más de 1 unidad de Rack.
15.10	Debe soportar un voltaje de entrada en el rango de 90 to 264 VAC.
15.11	Se requiere una tecnología de Stack Proporciona un sistema basado en virtualización del sistema, el cual forme un cluster en la capa de red que permita el comportamiento del cluster como si fuera una misma unidad de la solución en Alta Disponibilidad (HA), se debe interconectar mediante velocidad mínima de 40 Gbps, se deben proveer los componentes necesarios para dicho requerimiento.
15.12	Se requiere cumplimiento de seguridad MACsec-256.
15.13	La solución debe soportar los siguientes protocolos avanzados de enrutamiento: BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM SM, PIM SSM, PIM-BIDIR, IP SLA, OSPF.
15.14	Debe soportar las siguientes tecnologías de Segmentación de red; VRF, VXLAN, LISP, SGT, MPLS, mVPN.
15.15	Se requiere Soporte de Redes virtuales definidas por Software.
15.16	Soporte por lo menos de 81,000 MAC Address.
15.17	Mínimo 16G de memoria RAM y 16G de memoria Flash.
15.18	Debe integrarse de manera nativa con la plataforma de Switches Core existentes hoy en las instalaciones los cuales son unos Catalyst 9500.
15.19	Soporte minima de 1000 SVI.

15.20	Soporte mínimo de 1000 instancias de PVST.
15.21	Debe soportar mínimo 211,000 rutas IPv4.
15.22	Debe soportar mínimo 212,000 rutas IPv6.
15.23	Debe soportar mínimo 32,000 rutas Multicast.
15.24	Debe soportar al menos 4K VLANs.
15.25	Forwarding rate mínimo de 1 Bpps.
15.26	Soporte de Jumbo frames 9216 bytes.
15.27	Switching capacity mínimo de 2 Tbps.
15.28	Soportar las siguientes soluciones de Automatización: NETCONF, RESTCONF, gRPC, YANG, PnP Agent, ZTP/Open PnP, GuestShell (On-Box Python).
15.29	Se requiere que existan un mecanismo de detección para que un Switch monitoree y detecte si el otro switch par que conforma el cluster está disponible/activo o no debe realizarse sin el uso de un dispositivo intermediario, y que exista redundancia.
15.30	Requiere 3 cables con sus conectores 10GBASE-CU SFP+ Cable 3 Meter.
15.31	Requiere 3 cables con sus conectores 40GBASE-CR4 Passive Copper Cable, 5m.
15.32	Requiere 30 conectores 10GBASE-SR SFP Module.
15.33	Requiere 36 conectores 1000BASE-SX SFP transceiver module, MMF, 850nm, DOM.
15.34	50 Patch Cord de Fibra Óptica LC-LC OM4 de 3 metros.
15.35	50 Patch Cord de Fibra Óptica LC-LC OM4 de 5 metros.
15.36	30 Patch Cord de Fibra Óptica LC-LC OM4 de 10 metros.
15.37	No debe estar fuera de venta y/o vida por parte del fabricante. No puede ser reconstruido ni reparado.
15.38	Servicios de Soporte, Garantía y Mantenimiento por 36 meses con SLA Mínimo de 24X7X4.
16	***SWITCHES* DE ACCESO *DE OFICINA PRINCIPAL***
16.1	**Seis (10) Switches de Oficina Principal**
16.2	Administrable: Administrable vía CLI y vía una Plataforma de red Administrable por Software SDN. Requiere incluir las licencias para ser administrado de ambas manera.

16.3	Velocidad 10/100/1000 (PoE+) 24 Ports.
16.4	Uplink modular de interfaces 4 SFP+
16.5	Debe Soportar PoE+ 370W dedicado para PoE.
16. 6	Soporte de Power Supply Redundante para uso futuro.
16.7	Soporte de Stacking bandwidth mínimo de 288 Gbps.
16.8	Soporte por lo menos de 4 Redes virtuales definidas por Software.
16.9	Soporte por lo menos de 32,000 MAC Address.
16.10	Debe soportar mínimo 16,000 flujos de Netflow.
16.11	Mínimo 4 G de memoria RAM y 4 G de memoria Flash.
16.12	Debe integrarse de manera nativa con la plataforma de Switches Core existentes hoy en las instalaciones los cuales son unos Catalyst 9500.
16.13	Soporte mínimo de 1000 SVI.
16.14	Debe soportar al menos 4K VLANs.
16.15	Forwarding rate 95.23 Mpp.
16.16	Soporte de Jumbo frames 9198 bytes.
16.17	Switching capacity 128 Gbps.
16.18	Debe incluir soporte para las siguientes funcionalidades: IP SLA Responder, MACsec-128, PBR, EIGRP Stub, QoS.
16.19	Soportar las siguientes soluciones de Automatización: NETCONF, RESTCONF, YANG, PnP Agent, PnP.
16.20	No debe estar fuera de venta y/o vida por parte del fabricante. No puede ser reconstruido ni reparado.
16.21	Servicios de Soporte, Garantía y Mantenimiento por 12 meses con SLA mínimo de 8x5xNBD.
17	***SWITCHES DE ACCESO DE* OFICINAS REMOTAS**
17.1	Se deberán incluir 64 Switches de acceso, los cuales serán instalados en las diferentes dependencias del banco, ubicadas en las siguientes localidades as en todo el país."



	32 Sucursales: Santo Domingo, Higuey, San Cristóbal, Barahona, San Juan de la Mag., San Fco. de Macorís, Comendador, Cotuí, La Vega, Santiago Rodríguez, Montecristi, Puerto Plata, Nagua, Villa Riva, El Seíbo, Santiago, San José de Ocoa, Azua, Baní, Valverde Mao, Arenoso, Hato Mayor, Moca, Samaná, Bonao, Neyba, Dajabón, San José de las Matas, Río San Juan, Salcedo, Monte Plata, Constanza. **32 Oficinas de Negocios**: Padre las Casas, Enriquillo, Duverge, Sabana de la Mar, Jarabacoa, Gaspar Hernandez, Cabrera, La Isabela, Altamira, Luperón, Guananico, Janico, Partido, Loma de Cabrera, Yamasa, Miches, Pimentel, Villa Vásquez, Castillo, Las Matas de Farfán, Sanchez, Bohechio, Rancho Arriba, Las Matas de Santa Cruz, Fiscalía Sto Dgo Este, Tamayo, Hondo Valle, Sabana Grande de Boya, La Descubierta, La Romana, San Pedro, Fiscalía Santiago.
17.2	Administrable.
17.3	Velocidad 10/100/1000 (PoE+) 24 Ports.
17.4	Uplink interfaces 4 SFP.
17.5	Debe Soportar PoE+ 370W.
17.6	Debe integrarse de manera nativa con los firewalls existente en la oficina y que pueda administrase directamente desde ese mismo firewall.
17.7	Switching capacity 56Gbps.
17.8	Debe soportar al menos 4K VLANs.
4.09	Debe soportar conectividad segura para administración del equipo.
17.10	Debe soportar SSH, IPV6.
17.11	Debe soportar 8 Link Aggregation Groups.
17.12	Debe tener las siguientes certificaciones de cumplimiento: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2.
17.13	Oferente deberá configurar , instalar e integrar los equipos switch con las soluciones existentes y la central y los equipos propuestos.
17.14	No debe estar fuera de venta y/o vida por parte del fabricante. No puede ser reconstruido ni reparado.
17.15	Servicios de Soporte, Garantía y Mantenimiento por 36 meses con SLA mínimo de 24x7x4.
18	**CAPACITACION**

SECCIÓN DE COMPRAS Y CONTRATACIONES BAGRÍCOLA

18.1	Se deberá incluir 100 créditos de entrenamiento para capacitación de técnicos con certificación por parte del fabricante.
18.2	Se deberá incluir entrenamiento y transferencia de conocimiento para 2 técnicos por cada solución parte del oferente, las empresas participantes deben detallar la metodología y alcance con el cual impartirán este entrenamiento.
19	**REQUISITOS GENERALES DE LA OFERTA**
19.1	El suplidor de la solución debe estar acreditado Vigente como Partner Gold o Premier, o equivalente según la marca de la solución presentada. Estos datos serán comprobados con el fabricante.
19.2	Para la solución de SIEM, el suplidor de la solución debe estar acreditado vigente como Advantage, o equivalente según la marca de la solución presentada. Estos datos serán comprobados con el fabricante.
19.3	El Suplidor debe contar con la Certificación Vigente de Advanced Security Architecture Specialization o equivalente según la marca de la solución presentada. Estos datos serán comprobados con el fabricante. (Mostrar Evidencia).

SECCIÓN DE COMPRAS Y CONTRATACIONES
BAGRÍCOLA

DIONISIO E. JIMENEZ HDEZ.
Encargado Sección de Compras y Contrataciones