FICHA TÉCNICA CIBER EXPOSICIÓN	
Denominación Técnica:	Ciber exposición y Servicio de Exposición de Datos Filtrados, seguridad y gestión de vulnerabilidades.
Objeto: Adquirir una solución integral de Gestión de Ciberexposición y Servicio de Exposición de datos filtrados.	
Duración de la solución integral y demás servicios establecidos en la presente ficha técnica	Doce (12) meses.

Se relacionan a continuación los ítems solicitados para cotización, incluyendo su descripción técnica correspondiente:

1. GESTIÓN DE CIBEREXPOSICIÓN Y SERVICIO DE EXPOSICION DE DATOS FILTRADOS	
1.1	**Generalidades**
1.1.1	Se requiere una plataforma de gestión de ciber-exposición y como complemento un servicio continuo de análisis de filtrado de datos. La solución ofertada para Gestión de ciber-exposición deberá estar catalogada como una Plataforma de Exposición o ciber-exposición.
1.1.2	La solución ofertada de ciber-exposición deberá estar en la capacidad de abarcar la gestión de vulnerabilidades de las siguientes fuentes de información: Activos TI, Recursos Cloud, Contenedores, Aplicaciones Web y sistemas de identidad con la finalidad de priorizar acciones y comunicar el riesgo cibernético.
1.1.3	La solución ofertada permitirá tener una visión comprensiva de toda la superficie de ataque moderna.
1.1.4	La priorización de riesgos deberá basarse en un modelo de machine learning que analice por lo menos 150 variables y la amenaza en tiempo real, generando un puntaje de riesgo dinámico para enfocar los esfuerzos de remediación y prevenir ataques.
1.1.5	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades. El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio.
1.1.6	La solución ofertada permitirá comunicar el ciberiesgo para tomar mejores decisiones.
1.1.7	La solución ofertada permitirá conocer el nivel de exposición global de la organización.
1.1.8	La solución ofertada permitirá conoce de manera gráfica los posibles movimientos de un atacante basado en un análisis de riesgo utilizando el framework de MITRE ATT&CK.
1.1.9	La solución ofertada permitirá un control centralizado de activos sin importar la fuente de información (Activos TI, Recursos Cloud, Contenedores, Aplicaciones Web y sistemas de identidad).
1.1.10	La solución ofertada estará en la capacidad de integrarse con blogs de investigación del fabricante para la configuración de tarjetas de exposición personalizadas.

1.1.11	Se precisa que la información es propiedad de la entidad y por lo tanto mantendrá acceso a la información histórica, reportes y datos recolectados durante la vigencia de la licencia, aun si decide no renovar, en cuyo caso, el contratista deberá entregar un acta que certifique el borrado seguro de la información del IDU que haya sido recolectada en la solución ofertada.
1.1.12	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
1.2	**Nivel de Exposición**
1.2.1	La solución de Ciberexposición ofertada deberá evaluar y presentar el nivel de exposición de la organización teniendo en cuenta las siguientes fuentes de información: Activos TI, Recursos Cloud, Aplicaciones Web y Sistemas de identidad
1.2.2	La solución ofertada deberá evaluar y presentar el nivel de exposición de manera global.
1.2.3	La solución ofertada deberá evaluar y presentar el nivel de exposición por categorías.
1.2.4	El nivel de exposición se calculará teniendo en cuenta los siguientes factores: - Severidad y Explotabilidad de una vulnerabilidad. - Criticidad de un Activo. - Exposición de un Activo.
1.3	**Análisis de Ruta de Ataque.**
1.3.1	La plataforma deberá ser capaz de visualizar gráficamente las rutas de ataque que combinan vulnerabilidades, '*misconfiguraciones*' y problemas de identidad en activos de TI, nube y Directorio Activo, identificando los '*choke points*' o activos críticos que interrumpen más rutas de ataque si son remediados, basado en un análisis de riesgo utilizando el framework de MITRE ATT&CK
1.3.2	La solución ofertada tomará sus datos y los combinará con un análisis de gráficos avanzados y el framework de MITRE ATT&CK para crear hallazgos, dichos hallazgos permiten comprender y tomar acciones sobre situaciones desconocidas que permiten y amplifican el impacto en los activos e información de la entidad.
1.3.3	La solución ofertada permitirá realizar un análisis a profundidad permitiendo interactuar con la ruta de ataque, creando rutas personalizadas, de la misma forma manipular los orígenes y objetivos con la finalidad de observar de manera exacta como estos cambios afectan la información de la entidad
1.3.4	La solución ofertada deberá priorizar las rutas de ataque basado en: - Activos con ACR mayor a 7 - Rutas de ataque que conducen a activos críticos
1.3.5	La solución ofertada permitirá agrupar los hallazgos basado en su estado: - Hallazgos Abiertos - Hallazgos Archivados - Todos los hallazgos

1.3.6	La solución ofertada permitirá filtrar los hallazgos basado en: - Prioridad - Estado - Origen - Destino - CVEs - Mitigación - Táctica - Técnica
1.3.7	La solución ofertada permitirá exportar uno o más hallazgos en formato CVE incluyendo la siguiente información: - URL de Mitre - Estado - Conteo de Vector
1.3.8	La solución ofertada permitirá crear y ver y compartir comentarios en cualquier sección de la página de detalle del descubrimiento.
1.3.9	La solución ofertada permitirá cambiar el estado y archivar el descubrimiento.
1.3.10	La solución ofertada permitirá ver el detalle del descubrimiento incluyendo los siguientes campos: - Origen - Destino - Evidencia - Mitigación - Detección - Malware y Herramientas Relacionadas - Referencias
1.3.11	La solución ofertada permitirá compartir el descubrimiento por los siguientes medios: - URL - Correo Electrónico - Impresión
1.3.12	La solución ofertada permitirá observar los logs de los hallazgos, en los cuales se puede observar: - Cambio de estado (Open or Archived.) - Cambio en el estatus (To Do, In Progress, In Review, Or Done.) - Cambios en la prioridad (Critical, High, Medium, or Low)
1.3.13	La solución ofertada permitirá realizar un análisis a profundidad por medio de los siguientes mecanismos: - Query Builder para generar consultas personalizada - Blast Radius para visualizar las rutas de ataque de un activo o varios otros activos -Genere una consulta de gráfico de exposición de activos para visualizar rutas de ataque desde múltiples activos hasta un solo activo. - - Consulta integrada en la biblioteca de consultas para generar una consulta preconfigurada.

1.3.14	La solución ofertada deberá tener las siguientes consultas en su librería - Bookmarks - Active Directory Missconfiguration - Azure - Cloud Applications - Credentials - Endpoint - Exfiltration - Network - Permissions - Ransomware - Vectors
1.3.15	La solución ofertada deberá permitir observar gráficamente la ruta de ataque
1.4	**Acceso Administrativo de la Solución**
1.4.1	La solución ofertada deberá estar en la capacidad de gestionar los accesos a la aplicación por medio de RBAC (Role-Based Access Control), desde donde se puedan definir las actividades que un usuario puede ejecutar en un proyecto asociado a la consola.
1.5	**Inventario de Activos**
1.5.1	La solución ofertada permitirá ver y administrar fácilmente todos los activos una única ubicación independientemente del origen del activo.
1.5.2	La solución ofertada permitirá ver rápidamente que activos son nuevos o se han actualizado, de la misma forma conocer que porcentaje de activos proviene de que fuente individual.
1.5.3	La solución ofertada permitirá ver, administrar y aplicar etiquetas a los activos en el inventario.
1.5.4	La solución ofertada permitirá aplicar filtros a los activos consolidados en el inventario.
1.5.5	La solución ofertada permitirá personalizar las columnas de la vista de activos.
1.5.6	La solución ofertada permitirá ver el detalle de los activos en el inventario.
1.5.7	La solución ofertada permitirá ver los activos en el inventario con base a los tags asignados.
1.5.8	La solución ofertada permitirá cread, editar y eliminar tags.
1.5.9	La solución ofertada permitirá crear tags de manera estática y/o dinámica.
1.5.10	La solución ofertada permitirá ver el detalle de los tags.
1.6	**Soporte**

1.6.1	El fabricante de la herramienta debe proveer soporte 24 x 7 x 365
1.6.2	Los tiempos de respuesta inicial para problemas críticos debe ser de una hora o menos.
1.6.3	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
1.6.4	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II)
1.6.5	Implementación.
1.6.6	La solución debe proveerse como servicio en la nube.
1.6.7	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo a las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
2. ESCANEO DE VULNERABILIDADES	
2.1	**Generalidades**
2.1.1	Se requiere una solución de escaneo de vulnerabilidades, con el fin de visibilizar y priorizar todas las brechas de seguridad sobre la infraestructura. La cual cuente con una cobertura para 2200 activos por un periodo de 12 meses.
2.1.2	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio.
2.1.3	La solución ofertada deberá hacer parte de una plataforma de administración de exposición cibernética.
2.1.4	La solución ofertada deberá contar con una baja tasa de falsos positivos.
2.1.5	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.
2.2	**Gestión de Vulnerabilidades.**

2.2.1	Deberá realizar escaneo de vulnerabilidades de sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores Web e infraestructuras esenciales para las vulnerabilidades y las infracciones de cumplimiento.
2.2.2	La solución debe proporcionar una consola de gestión on-premises para la gestión de la información de seguridad.
2.2.3	La solución deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de: -Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Dicha tecnología deberá estar patentada. -Los sensores de monitoreo pasivo deben tener la capacidad de ser desplegados en modalidad de alto desempeño para el monitoreo de enlaces de 10 GB. -Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes.
2.2.4	Los sensores deben poder desplegarse en una variedad de plataformas, incluyendo: Windows Workstations y Servers, Linux, Mac OS ya sea en dispositivos virtuales o físicos.
2.2.5	El servicio deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad. Dicha calificación deberá ser obtenida a partir de los siguientes factores: -La priorización deberá correlacionar información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación. -El modelo de priorización deberá ser capaz de predecir si una vulnerabilidad tiene posibilidades de explotación en el futuro cercano. -La priorización deberá considerar elementos de evaluación diversos, como: edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, número de días desde que se conoció una actividad de amenaza sobre la vulnerabilidad.
2.2.6	La solución deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo.
2.2.7	La solución deberá poder equilibrar cargas a través de múltiples escáneres de forma dinámica con base en la disponibilidad de cada escáner desplegado.
2.2.8	La solución deberá proveer una vista de soluciones que permitan enfocar en las secciones más importantes primero. Dicha vista deberá proveer los siguientes datos: -Descripción de la solución. -Número de dispositivos asociados a la solución. -Número de instancias de vulnerabilidades asociadas a la solución. -La calificación dinámica de probabilidad de explotación más alta para las vulnerabilidades asociadas a la solución.
2.2.9	La solución debe soportar direcciones IP sobrepuestas.
2.2.10	La solución solicitada deberá incluir la posibilidad de programar ventanas de escaneo.
2.2.11	Poder etiquetar los activos por grupos en función de las necesidades de la organización para poder categorizar los resultados y asignar las tareas correspondientes. El etiquetado deberá poder realizarse de forma manual y dinámica, basado en atributos del activo (ej. Sistema Operativo, software instalado)

	o en reglas de negocio (ej. criticidad del activo). La plataforma deberá contar con una métrica de Criticidad de Activos (ACR) que se ajuste automáticamente según reglas configurables.
2.2.12	La solución debe permitir proveer un esquema de perfiles de usuarios basados en funciones de trabajo y los niveles adecuados de acceso a la funcionalidad.
2.2.13	La solución deberá contar con una bóveda de contraseñas para ser gestionadas de manera central.

2.2.14	La solución debe soportar múltiples sets de credenciales Windows, SSH y SNMPv3.
2.2.15	La solución debe permitir la autenticación hacia diferentes servicios en la nube para aplicar escaneos de vulnerabilidades o de auditoría. Los servicios contemplados en esta característica deben ser al menos los siguientes: AWS, Microsoft Azure, Office 365. Rackspace y Salesforce.
2.2.16	Contar con un módulo que permita la creación de filtros para mejorar las búsquedas. Estos filtros deberán poder ser por lo menos: protocolo, IP, activo, identificador de la vulnerabilidad, identificador CVE, CVSS, vulnerabilidades por su puntaje dinámico, explotabilidad, severidad.
2.2.17	La solución deberá poder guardar estos filtros para reutilizarlos cuando se requieran.
2.2.18	La solución deberá permitir clasificar a los activos identificados de manera manual o dinámica, con base en diferentes atributos encontrados en el análisis con base en etiquetas o en grupos de trabajo, para poder usarse en escaneos posteriores.
2.2.19	Deberá contar con un API que permita hacer integraciones programáticas y con otras soluciones para intercambio de información.
2.2.20	La solución debe proporcionar información de capacidad de explotación contra las plataformas de validación como Metasploit, CoreImpact y Canvas.
2.2.21	La solución deberá permitir la personalización de auditorías de configuraciones de acuerdo con la necesidad de la entidad. Estas personalizaciones deberán estar basadas en expresiones regulares especificadas en archivos que permitan validar la configuración, permisos de archivos y pruebas de controles de acceso a revisar. Los valores por comparar deberán poderse ajustar con base en las guías de configuración de la entidad.
2.2.22	La solución debe ser capaz de proporcionar información de reputación en procesos encontrados y fuentes de inteligencia de amenazas para búsqueda de malware.
2.2.23	La solución deberá poder configurar reglas de escaneo con soporte de reglas YARA.
2.2.24	La solución debe soportar un segundo factor de autenticación.
2.2.25	La solución debe soportar autenticación compatible con sistemas basados en SAML 2.0 como OKTA o One Login.
2.2.26	Debe soportarse autenticación basada en Shibboleth 1.3.

2.2.27	La solución deberá tener la capacidad de simular ejercicios de explotación benignos para algunas de las vulnerabilidades identificadas a fin de confirmar la presencia y explotabilidad de las mismas.
2.3	**Compliance**
2.3.1	El servicio debe proporcionar la capacidad de ejecutar escaneos de auditoría de cumplimiento de configuraciones usando plantillas incluidas por defecto al menos para los siguientes tipos de sistemas: Adtran AOS, Alcatel TiMOS, Amazon AWS, Arista EOS, Blue Coat Proxy SG, Brocade Fabric OS, Check Point GAiA, Cisco ACI, Cisco Firepower, Cisco IOS, Citrix XenServer, Database, Dell Force10 FTOS, Extreme XOS, F5. FireEye, Fortigate Forti OS, HP Procurve, Huawei VRP, IBM iSeries, Juniper Junos, Microsoft Azure, Mobile Device Manager, Mongo DB, NetApp API, Office 365. OpenStack, NetApp Data ONTAP, PAN OS, Rackspace, RHEV, Salesforce.com, SonicWall SonicOS, Unix, VMWare vCenter/vSphere, Watchguard, Windows, ZTE Rosng.
2.3.2	La solución deberá permitir el uso de archivos de auditoria construidos por el usuario para evaluar la configuración de sistemas Unix, Windows, bases de datos, SCADA, IBM iSeries y Cisco.
2.3.3	La solución debe proporcionar por defecto plantillas de auditoria basadas en la política de cumplimiento de auditorías de CIS.
2.3.4	La solución debe proporcionar por defecto archivos de auditoría de PCI para sistemas AIX, HP-UX, Linux, Solaris y Windows.
2.3.5	La solución debe proporcionar por defecto plantillas de auditoría para políticas basadas en SCAP para el cumplimiento de requerimientos de DISA STIG, NIST, entre otras.
2.4	**Performance**
2.4.1	La solución debe ser capaz de deshabilitar toda actividad que pueda tener un efecto adverso en el activo escaneado.
2.4.2	Con el fin de reducir el tráfico innecesario en la red, la solución debe ser capaz de detener el escaneo en activos que dejen de responder los intentos de comunicación.
2.4.3	El escáner utilizado por la solución debe ser capaz de reducir la demanda del escaneo cuando detecte congestión en la red.
2.4.4	Debe tenerse la capacidad de definir un número máximo de segundos que el escáner de la solución pueda esperar por una respuesta del activo a escanear.
2.4.5	Debe tenerse la capacidad de establecer el número máximo de validaciones que pueden aplicarse simultáneamente en un activo escaneado.
2.5	**Integraciones**

2.5.1	La solución debe tener la capacidad de integrarse con sistemas tipo SIEM para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a vulnerabilidades. Por defecto debe tener la capacidad de integrarse al menos con las siguientes soluciones: Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic
2.5.2	Capacidad de integrarse con soluciones MDM para identificación de vulnerabilidades en dispositivos móviles, por lo menos: VMWare Workspace One, Apple Profile Manager, MaaS360, Blackberry, Microsoft Intune y MobileIron.
2.5.3	La solución debe tener la capacidad de integrarse con soluciones tipo Privileged Access Management (PAM), pudiendo hacerlo de forma nativa al menos con los siguientes fabricantes: Arcon, Beyond Trust, Centrify, Cyber Ark, Hashi Corp, Thycotic.
2.5.4	La solución debe proporcionar una integración con los sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Por lo menos se deben soportar: Microsoft WSUS/SCCM, Red Hat Satellite, HCL BigFix, Symantec Altiris, Dell KACE K1000.
2.5.5	Deberá contar con un conector específico para el servicio de Amazon Web Services, Microsoft Azure y Google Cloud Platform que permitan importar los activos existentes en estos servicios de nube pública.
2.5.6	Cuando un activo sea descubierto por el conector de AWS, Azure o GCP, no debe contar automáticamente contra la licencia de la solución a menos que sean escaneados posteriormente para descubrir sus vulnerabilidades.
2.5.7	Para el servicio de nube pública de AWS la plataforma debe ser capaz de ejecutar análisis de vulnerabilidades sin la necesidad de usar un escáner, agente o algún otro mecanismo intrusivo en la red privada virtual.
2.6	**Reportes y Dashboards**
2.6.1	La solución debe proporcionar dashboards por default que puedan ser exportados al menos en los siguientes formatos: PDF, PNG y JPG.
2.6.2	Dashboards que deberán desplegar los datos históricos basados en la versión de CVSS configurada al momento de que los datos fueron calculados.
2.6.3	La solución deberá poder exportar información en formatos PDF, HTML y CSV.
2.6.4	Los dashboards deberán poder mostrar la tendencia de identificación de vulnerabilidades y su evolución con el paso del tiempo, mostrando la información relevante de las vulnerabilidades.
2.6.5	Los dashboards deberán permitir filtros editables a aplicar en función de los grupos de activos de la organización, ser editables y agregar búsquedas personalizadas.

2.6.6	Los dashboards deberán ser personalizables mediante la capacidad de agregar distintos componentes como: tablas, matrices, gráficas de línea, gráficas circulares, gráficas de barras y gráficas de área.
2.6.7	Los dashboards deberán poderse exportar en formato PDF, así como poderse programar las exportaciones de acuerdo con las necesidades del administrador.
2.7.	**Transferencia de Conocimiento**
2.7.1	Realizar una capacitación especializada por el fabricante a nivel de la solución ofertada como mínimo para 2 integrantes del equipo de seguridad de la entidad.
2.8	**Implementación**
2.8.1	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada.
2.8.3	La solución debe proveerse como servicio en la nube
2.8.4	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
3. ESCANEO DE APLICACIONES WEB	
3.1	**Generalidades**
3.1.1	Se requiere una solución de escaneo de aplicaciones web, con el fin de visibilizar todas las vulnerabilidades sobre los sitios web y aplicaciones basadas en Rest. La cual cuente con una cobertura para 100 FQDN por un periodo de 12 meses
3.1.2	La solución ofertada deberá hacer parte de una plataforma de administración de exposición cibernética.
3.1.3	La solución ofertada deberá contar con una baja tasa de falsos positivos.
3.1.4	La solución ofertada deberá poder escanear aplicaciones modernas desarrolladas en frameworks JavaScript, AJAX, HTML5 and Single Page Applications.
3.1.5	La solución ofertada deberá entregar resultados de escaneos de seguridad en dos minutos o menos.
3.1.6	La solución ofertada permitirá observar las vulnerabilidades a lo largo del tiempo, según su nivel de riesgo, clasificación en OWASP Top 10. de la misma forma que sus descripciones e instrucciones de remediación.

3.1.7	La solución ofertada deberá contar con dashboards predefinidos y permitir la creación de dashboards personalizados.
3.1.8	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio
3.1.9	La solución ofertada permitirá realizar escaneos sin degradación de performance en el sitio, por medio de escaneos seguros, permitiendo definir sitios que no deben ser escaneados a partir de la URL, o extensiones de archivos.
3.1.10	La solución ofertada deberá permitir automatización en procesos de escaneos de aplicaciones web.
3.1.11	La solución ofertada deberá contar con dos escaneos predefinidos que permitan detectar rápidamente problemas de ciber higiene: - SSL/TLS Scan - Config Audit Scan
3.1.12	La solución ofertada deberá permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.
3.1.13	La solución ofertada soportar escaneos con autenticación avanzada como: - form-based authentication - cookie-based authentication - NTLM support - Selenium-based authentication
3.1.14	La solución ofertada deberá soportar integraciones vía API y las mismas deben estar documentadas.
3.1.15	La solución ofertada deberá ser tipo SaaS, de la misma forma tendrá capacidad para ser desplegada como un contenedor de Docker. La información sensible de la entidad (activos, vulnerabilidades, configuraciones) debe ser alojada y procesada dentro de centros de datos ubicados en Colombia o en países que cumplan con estándares de protección de datos equivalentes o superiores a la Ley Estatutaria No. 1581 de 2012 y otros lineamientos del MinTIC.
3.1.16	La solución debe permitir observar el estado de licenciamiento de la plataforma.
3.1.17	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
3.1.18	El contratista deberá entregar hojas de datos (datasheets) o manuales del fabricante evidenciando cumplimiento de la solución.

3.1.19	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.
3.2	**Escaneos**
3.2.1	La solución ofertada deberá contar con scaners cloud.
3.2.2	La solución ofertada permitirá el escaneo de sitios web públicos y privados.
3.2.3	La solución ofertada deberá contar con las siguientes plantillas de escaneo: - Scan - Overview - PCI - SSL/TLS - Config Audit - API Scan
3.2.4	La solución ofertada deberá contar con validaciones rápidas a nivel de superficie: - Untuned Detailed Scans - Authenticated Detailed Scans - Tuned Detailed Scans
3.2.5	La solución ofertada permitirá crear, configurar, lanzar y administrar escaneos web.
3.2.6	La solución ofertada permitirá observar un resumen y de manera detallada el resultado de una tarea de escaneo.
3.2.7	La solución ofertada permitirá exportar el resultada de una tarea de escaneo en los siguientes formatos: HTML, PDF, Nessus, CSV, JSON y ZIP.
3.2.8	La solución ofertada permitirá conocer el estado y el progreso de una tarea de escaneo.
3.2.9	La solución ofertada permitirá calendarizar las tareas de escaneo.
3.2.10	La solución ofertada permitirá enviar los resultados de los escaneos vía correo electrónico.
3.2.11	La solución ofertada permitirá definir un scope para los escaneos: - Crawl Script - OpenAI Specification - Scan Inclusion - Scan Exclusion

3.2.12	La solución ofertada permitirá auditar los siguientes elementos: - Cookies - Headers - Forms - Links and Query String Parameters - Parameter Names - Parameter Values - Path Parameters - JSON Elements / Request Body (JSON) - XML Elements / Request Body (XML) - UI Forms - UI Inputs
3.2.13	La solución ofertada deberá permitir los siguientes mecanismos de autenticación: - HTTP Server Authentication - Web Application Authentication (Login Form, Cookie Authentication, Selenium Authentication, API Key, Bearer Authentication) - Client Certificate Authentication

3.2.14	La solución ofertada deberá poseer las siguientes plantillas de escaneo: - API - Config Audit - log4Shell - Overview - PCI - Quick Scan - Scan - SSL/TLS
3.2.15	La solución ofertada deberá permitir la creación de templetes personalizados.
3.3	**Acceso Administrativo de la Solución**
3.3.1	La solución ofertada deberá estar en la capacidad de gestionar los accesos a la aplicación por medio de RBAC (Role-Based Access Control), desde donde se puedan definir las actividades que un usuario puede ejecutar en un proyecto asociado a la consola.
3.4	**Dashboards**
3.4.1	La solución ofertada deberá contar con dashboards predefinidos y permitir la creación de dashboards personalizados.

4.4.2	La solución ofertada deberá contar con los siguientes widgets: - Finding - Web Assets Scanned - Incomplete Scans - Non Authenticated Scans - OWASP Top 10
3.5	**Activos**
3.5.1	La solución ofertada deberá contar con la capacidad de rastrear activos.
3.5.2	La solución ofertada creará y actualizará los activos de manera automática al momento de concluir el escaneo.
3.5.3	La solución ofertada permitirá observar la siguiente información en los dominios o aplicaciones descubiertos: - Asset ID - Name - Host Name - Record Type - Record Value - Domain - DNS (FQDN) - IP Address - Hosting Provider - ASN - Hosting Provider - Created Date - Updated Date - Port - Actions
3.5.4	La solución ofertada permitirá observar la siguiente información en las aplicaciones escaneadas: - Name - AES - ACR - SSL/TLS - IPv4 Address - Operating System - Last Seen - Source - Tags - Actions

3.5.5	La solución ofertada permitirá observar un resumen de los dominios o aplicaciones: - Header - Asset Exposure Score - Asset Criticality Rating - Screenshot Available - Asset Information - Scan Information - License Information - Tags - Custom Attributes
3.5.6	La solución ofertada permitirá observar el detalle de los dominios o aplicaciones: - Header - Asset Information - Additional Information - Findings - Asset Exposure Score - Asset Criticality Rating - Tags - Web Application Findings - Scan Information

3.5.7	La solución ofertada deberá permitir el uso de los siguientes filtros a las aplicaciones escaneadas: - ACR - ACR Severity - AES - AES Severity - Asset ID - Custom Attribute - Last Authenticated Scan - Scan - Last Seen - Licensed - Mitigated - Mitigation Last Detected - Mitigation Product Name - Mitigation Version - Name - Operating System - Scanned vs. Discovered - SSL/TLS - Tags
3.5.8	La solución ofertada deberá permitir el uso de los siguientes filtros a los dominios descubiertos: - ASN - Asset ID - Created Date - Deleted - DNS (FQDN) - Domain - Host Name - Hosting Provider - IPv4 Address - IPv6 Address - Name - Port - Record Type - Tags - Updated Date
3.5.9	La solución ofertada podrá eliminar activos y prevenir activos duplicados.
3.5.10	La solución ofertada podrá exportar el listado de activos en formato CVS o JSON.

3.5.11	La solución ofertada podrá exportar el detalle de un activo determinado en formato CVS o JSON.
3.6	**Hallazgos**
3.6.1	La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura.
3.6.2	La solución ofertada permitirá observar la siguiente información en los hallazgos de vulnerabilidades: - Asset Name - Severity - Name - Plugin ID - Family - State - Last Update - Asset ID - First Seen - Actions
3.6.3	La solución ofertada permitirá observar la siguiente información del resumen de los hallazgos de vulnerabilidades: - Header - Asset Information - Vulnerability Information - Reference Information - Overview - Plugin Output - Attachments
3.6.4	La solución ofertada permitirá observar la siguiente información en los detalles de los hallazgos de vulnerabilidades: - Description - Solution - See Also - Asset Information - Identification - Http Info - Attachments - Finding State - Vulnerability Information - Discovery - Scan Information - Plugin Details - Risk Information - Reference Information

3.6.5	La solución ofertada permitirá agrupar los hallazgos por: - Assets - Plugins

3.6.6	La solución ofertada permitirá utilizar los siguientes filtros sobre la tabla de hallazgos: - Asset ID - Asset Name - Bugtraq ID - CPE - CVE - CVSSv2 Base Score - CVSSv2 Vector - CVSSv3 Base Score - CVSSv3 Vector - CWE - First Seen - Input Name - Input Type - Last Observed - Original Severity - OWASP 2010 - OWASP 2013 - OWASP 2017 - OWASP 2021 - OWASP API 2019 - Plugin Description - Plugin Family ... continua - Plugin ID - Plugin Modification Date - Plugin Name - Plugin Published - Risk Modified - Severity - Solution - State - URL - WASC
3.6.7	La solución ofertada permitirá exportar los hallazgos en formato CSV y JSON.
3.6.8	La solución ofertada permitirá exportar el detalle de los hallazgos en formato CSV y JSON.
3.6.9	La solución ofertada permitirá crear reglas de recast y aceptación.
3.6.10	La solución ofertada permitirá guardar, editar, eliminar, compartir y aplicar filtros para una fácil reutilización.

3.6.11	La solución ofertada permitirá guardar, editar, exportar y eliminar las tablas de hallazgos filtradas.

3.7	**Implementación**
3.7.1	La solución debe proveerse como servicio en la nube.
3.7.2	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
3.7.3	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
3.8	**Soporte**
3.8.1	El fabricante de la herramienta debe proveer soporte 24 x 7 x 365.
3.8.2	Los tiempos de respuesta inicial para problemas críticos debe ser de una hora o menos.
3.8.3	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
3.8.4	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
4. SEGURIDAD SUPERFICIE DE ATAQUE EXTERNA	
4.1	**Generalidades**
4.1.1	Se requiere una solución de auditoría y monitoreo para toda la superficie de ataque externa de la organización, con el fin de visibilizar todos los activos conectados a internet de manera dinámica y obtener información de seguridad e infraestructura de los que se encuentran incluidos y no limitados a puertos expuestos, vulnerabilidades, tipo de servidores y versiones. La cual cuente con una cobertura para 120 activos por un periodo de 12 meses.
4.1.2	La solución ofertada deberá estar clasificada como una herramienta de clasificación de activos web, que permita la identificación de activos conocidos y desconocidos.
4.1.3	La solución ofertada deberá hacer parte de una plataforma de administración de exposición cibernética.

4.1.4	La solución ofertada deberá identificar activos basado en: - Registros DNS - Direcciones IP - ASN
4.1.5	La solución ofertada deberá tener la capacidad de obtener información sobre la superficie de ataque en cuestión de minutos.
4.1.6	La solución ofertada deberá categorizar los activos descubiertos con base en un modelo de datos enriquecido (más de 200 campos de metadatos). De manera fundamental, la plataforma deberá proporcionar, para cada activo, una razón de atribución clara y auditable que explique la evidencia por la cual se le vincula a la organización, permitiendo así una validación rápida y transparente de los resultados.
4.1.7	La solución ofertada deberá tener la capacidad de monitorear y notificar los cambios sobre los activos expuestos a internet de manera periódica: diaria o semanal.
4.1.8	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio
4.1.9	La solución ofertada deberá tener la capacidad de lanzar escaneos de vulnerabilidades y escaneos de sitios web de los activos descubiertos.
4.1.10	La solución ofertada deberá estar en la capacidad de descubrir dominios relacionados a los activos identificados y clasificados en el inventario de la solución, suministrando razones del porque el dominio debería ser parte de la organización.
4.1.11	La solución ofertada deberá tener la capacidad de administrar los activos de la organización, permitiendo el uso de filtros, tags y tipo de datos.
4.1.12	La solución ofertada deberá soportar integraciones vía API y las mismas deben estar documentadas
4.1.13	La solución ofertada deberá tener la capacidad de integrarse con las demás soluciones del fabricante, incluida la solución de seguridad del directorio activo.
4.1.14	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
4.1.15	El contratista deberá entregar hojas de datos (datasheets) o manuales del fabricante evidenciando cumplimiento de la solución.

4.1.16	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.
4.2	**Acceso Administrativo de la Solución**
4.2.1	Para el acceso administrativo a la plataforma se debe permitir la integración con servidores LDAP, uso de SAML o cuentas creadas internamente.
4.2.2	La herramienta debe permitir la creación de perfiles para personalizar los datos presentados de acuerdo con el rol de la persona que acceda a la consola de administración.
4.2.3	La herramienta debe proporcionar un registro de toda la actividad administrativa realizada sobre la consola con fines de auditoría.
4.2.4	La solución debe restringir el acceso a los datos y opciones administrativas por medio de la creación de roles personalizados.
4.2.5	La solución ofertada deberá contar con un portal de administración que permita llevar acabo las siguientes actividades: - Ver y editar la lista de usuarios de la organización - Agregar y remover inventarios a cuentas de usuarios - Cambiar los límites de activos para un inventario especifico o para la totalidad de inventarios - Crear nuevos inventarios - Modificar el rol del usuario - Deshabilitar usuarios
4.3	**Inventarios**
4.3.1.	La solución ofertada deberá identificar activos basado en: - Registros DNS - Direcciones Ips - ASN - Autonomous System Number - Fuentes de Cloudflare
4.3.1.	La solución ofertada deberá estar en la capacidad de descubrir dominios y subdominios para la construcción del inventario.
4.3.1.	La solución ofertada deberá estar en la capacidad de aplicar filtros al inventario de activos.
4.3.1.	La solución ofertada deberá estar en la capacidad de guardar uno o más filtros como subscripciones, permitiendo consultas dinámicas sobre los activos que hacen match.
4.3.1.	La solución ofertada deberá estar en la capacidad de identificar cambios en los activos del inventario.

4.3.1.	La solución ofertada deberá estar en la capacidad de mover activos entre inventarios.
4.3.1.	La solución ofertada deberá estar en la capacidad de generar screenshots de los sitios que dispongan un portal web, de la misma forma que la actualización de este.
4.3.1.	La solución ofertada deberá estar en la capacidad de remover activos del inventario.
4.3.1.	La solución ofertada deberá estar en la capacidad de crear reglas de excepción para la no identificación de activos.
4.3.1.	La solución ofertada deberá estar en la capacidad de generar reglas automatizadas para los siguientes casos de uso: - Archivar Activos - Modificar Tags - Actualizar columnas personalizadas - Sugerencias - Mover Activos - Correr consulas ad-hoc

4.3.1.	La solución ofertada deberá permitir consultar los detalles de los activos permitiendo ver: - Detalles de Redes - Detalles de Servicios - Detalles de SSL/TLS - Detalles de Ubicación - Detalles de HTTP
4.3.1.	La solución ofertada deberá estar en la capacidad de exportar activos.
4.4	**Notificaciones**
4.4.1	La solución ofertada deberá estar en la capacidad de notificar los cambios que se presenten sobre los activos del inventario por medio de los siguientes medios: - Correo Electrónico - Slack - ServiceNow
4.5	**Sugerencia de Dominios**
4.5.1	La solución ofertada deberá estar en la capacidad de descubrir dominios relacionados a los activos identificados y clasificados en el inventario de la solución, suministrando razones del porque el dominio debería ser parte de la organización.
4.5.2	La solución ofertada permitirá incorporar un dominio sugerido al inventario.

4.5.3	La solución ofertada permitirá excluir dominios de los dominios sugeridos mediante blocklist, permitiendo agregar: - Domain names - Email addresses - Hostname - CIDR
4.5.4	La solución ofertada permitirá sugerir dominios basado en: - Domain names basados en los activos del inventario - Nombre de Marcas - Email addresses, - Nombre de Organizaciones - Nameservers - Backref links
4.6	**Subscripciones**
4.6.1	La solución ofertada permitirá el uso de subscripciones con el fin de notificar cambios sobre la superficie de ataque, incluyendo: - Identificación de nuevos servidores - Nuevos puertos abiertos o cerrados - Nuevo Software

4.6.2	La solución ofertada contará con las siguientes subscripciones predefinidas: - Compliance - Expposición - Geografía - Higiene TI - Marketing - tecnología
4.6.3	La solución ofertada deberá estar en la capacidad de crear, compartir, copiar y borrar subscripciones personalizadas.
4.7	**Dashboards**
4.7.1	La solución ofertada deberá contar con dashboards para mejor entendimiento de la información obtenida.
4.8	**Implementación**
4.8.1	La solución debe proveerse como servicio en la nube.

4.8.2	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
4.8.3	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
4.9	**Soporte**
4.9.1	El fabricante de la herramienta debe proveer soporte 24 x 7 x 365.
4.9.2	Los tiempos de respuesta inicial para problemas críticos debe ser de una hora o menos.
4.9.3	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
4.9.4	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
5. SEGURIDAD EN LA NUBE PUBLICA	
5.1	**Generalidades**
5.1.1	La solución ofertada deberá proporcionar una Plataforma de Protección de Aplicaciones Nativas en la Nube (CNAPP) nativamente unificada y provista por un único fabricante. Dicha plataforma deberá integrar, como mínimo, las siguientes capacidades en una única consola y bajo un modelo de datos correlacionado: Gestión de la Postura de Seguridad en la Nube (CSPM), Protección de Cargas de Trabajo en la Nube (CWPP), Gestión de Derechos de Infraestructura en la Nube (CIEM) y Seguridad de Infraestructura como Código (IaC). La solución deberá demostrar la capacidad de correlacionar hallazgos entre estos distintos módulos para identificar y priorizar rutas de ataque complejas en el entorno de nube. La cobertura mínima requerida es de 50 activos por un periodo de 12 meses.

5.1.2	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio
5.1.3	La solución ofertada deberá hacer parte de una plataforma de administración de exposición cibernética.
5.1.4	La solución ofertada deberá contar con una baja tasa de falsos positivos.
5.1.5	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.

5.2	**Inventario de Activos**
5.2.1	La solución debe ser capaz de proveer un inventario de activo sobre múltiples proveedores de nube/cuentas/regiones/servicios
5.2.2	La solución debe proveer visibilidad de todos los tipos de recursos, incluidos IAM, computación, datos, redes, contenedores, monitoreo, bitácoras, secrets y claves.
5.2.3	La solución debe permitir filtrar recursos según la estructura organizativa, tipo, nombre, recursos vinculados, etiquetas, exposición, etc.
5.2.4	La solución debe permitir búsqueda global basada en el nombre del recurso, dirección IP, clave de acceso, secreto, certificado, etc.
5.2.5	La solución debe proveer visibilidad de la configuración de recursos y los metadatos.
5.2.6	La solución debe proveer visibilidad de los permisos otorgados para cada recurso.
5.2.7	La solución debe proveer visibilidad de la actividad en la nube relacionada con cada recurso (creación, acceso, modificación).
5.2.8	La solución debe proveer visibilidad de los permisos de identidad en entornos múlti nubes.
5.2.9	La solución debe proveer visibilidad de las configuraciones erróneas asociadas a cada recurso.
5.2.10	La solución debe proveer visibilidad de la accesibilidad a tareas de la red para recursos expuestos.
5.2.11	La solución debe proveer visibilidad de permisos otorgados (que puede hacer y acceder) a identidades en la nube (service principals y humanos) y su uso.
5.2.12	La solución de ser capaz de proveer un inventario de activos para proveedores de identidades federados (IdPs): usuarios, grupos, roles, aplicaciones (por ejemplo, Okta, Ping, OneLogin, Azure AD).
5.2.13	La solución debe permitir crear snapshots de la configuración de permisos en la nube.
5.2.14	La solución debe permitir explorar las relaciones entre entornos, identidades y recursos vinculados.
5.2.15	La solución debe permitir etiquetar recursos sensitivos.
5.2.16	La solución debe permitir etiquetar recursos basados en las cloud tags
5.2.17	La solución debe ser capaz de detectar propietarios de los recursos según la actividad.
5.2.18	La solución debe permitir exportar la información del inventario de activos.
5.2.19	La solución debe permitir generar informes periódicos de inventario de activos para auditorías.

5.3	**Configuraciones Erróneas**
5.3.1	La solución debe ser capaz de detección de configuraciones incorrectas de la nube en todos los tipos de recursos en un ambiente multi-nube.
5.3.2	La solución debe ser capaz de detección de configuraciones erróneas relacionadas con IAM, computación, red, datos, seguridad, etc.
5.3.3	La solución debe proveer priorización de riesgos basada en información contextual (por ejemplo, exposición de la red, permisos otorgados (que puede hacer y acceder)).
5.3.4	La solución debe proporcionar el correctivo recomendado para los hallazgos de configuraciones erróneas de la nube.
5.3.5	La solución debe proveer la capacidad de resolver automáticamente los hallazgos asociados con configuraciones erróneas de la nube.
5.3.6	La solución debe proveer la capacidad de crear políticas de evaluación de configuraciones personalizadas.
5.4	**Cumplimiento**
5.4.1	La solución debe capaz de evaluar la postura de seguridad en la nube basado en las mejores prácticas de la industria (por ejemplo, CIS Benchmark para AWS/Azure/GCP, AWS Well-architected).
5.4.2	La solución debe capaz de evaluar la postura de seguridad en la nube según los marcos y estándares de cumplimiento de la industria (e.g. SOC2. HIPAA, NIST, GDPR, PCI-DSS, NYDFS).
5.4.3	La solución debe proporcionar puntuación de cumplimiento para cada estándar, así como para los controles subyacentes.
5.4.4	La solución debe proveer la capacidad de crear políticas de evaluación de cumplimiento personalizadas.
5.4.5	La solución debe permitir generar informes de cumplimiento para unidades organizativas específicas (OU, carpeta, grupo de cuentas, etc.).
5.4.6	La solución debe permitir generar informes de cumplimiento para una organización completa.
5.4.7	La solución debe permitir generar informes de cumplimiento automáticamente según a cadencia preestablecida.

5.5	**Recursos en Riesgo (Expuestos).**
5.5.1	La solución debe identificar recursos expuestos públicamente en entornos de múltiples nubes.

5.5.2	La solución debe identificar recursos expuestos externamente (acceso entre cuentas/organizaciones).
5.5.3	La solución debe identificar recursos computacionales y de datos accesibles desde Internet (exposición de la red).
5.5.4	La solución debe proveer cobertura completa de recursos e identidades públicamente expuestos.
5.5.5	Uso Seguro de secrets and keys.
5.5.6	La solución debe proveer visibilidad total en un entorno multi-nube de keys, secrets, certificados y claves de acceso.
5.5.7	La solución debe proveer un diagrama de los derechos sobre secrets, keys, etc.
5.5.8	La solución debe identificar los keys y secrets expuestos públicamente.
5.5.9	La solución debe ser de identificar secrets en textos sin cifrar (cleartext) almacenados en variables de ambiente, scripts de inicio de VM, etiquetas, configuración, etc.
5.5.10	La solución debe ser capaz de detectar keys/secrets no rotados (usuarios de IAM, cuentas de servicio, registros de aplicaciones, etc.)
5.5.11	La solución debe ser capaz de detectar accesos inusuales a secrets y keys.
5.6	**Proveedores de Identidad (IdP)**
5.6.1	La solución debe permitir la integración basada en API con proveedores de identidades para una visibilidad completa de los derechos en la nube.
5.6.2	La solución debe proveer - Soporte total para Google Workspace.
5.6.3	La solución debe proveer - Soporte total para Azure Active Directory.
5.6.4	La solución debe proveer - Soporte total para AWS SSO.
5.6.5	La solución debe proveer - Soporte total para OneLogin.
5.6.6	La solución debe proveer - Soporte total para Okta.
5.6.7	La solución debe proveer - Soporte total para Ping.
5.6.8	La solución debe identificar usuarios y grupos privilegiados.
5.6.9	La solución debe proveer un diagrama de los derechos de usuarios y grupos corporativos.

5.6.10	La solución debe identificar permisos excesivos de usuarios y grupos corporativos.

5.7	**Gobernanza de Riesgos de IAM**
5.7.1	La solución debe proveer visibilidad total de las identidades y sus derechos.
5.7.2	La solución debe proveer soporte para AWS: IAM Users, Groups, Roles, AWS SSO Users/Groups/PermissionSets.
5.7.3	La solución debe proveer soporte para Azure: Users, groups, group membership, applications, managed identities (system and user-managed).
5.7.4	La solución debe proveer soporte para GCP: Users, Groups, Domains, Service Accounts.
5.7.5	La solución debe detectar identidades asumibles por instancias informáticas e identidades externas.
5.7.6	La solución debe proveer visibilidad total de las identidades federadas (usuarios, grupos, aplicaciones, etc.).
5.7.7	La solución debe proveer visibilidad de los permisos otorgado a los recursos.
5.7.8	La solución debe proveer visibilidad de permisos otorgados entre nubes.
5.7.9	La solución debe proveer soporte total para políticas basadas en identidad.
5.7.10	La solución debe proveer soporte total para políticas basadas en recursos.
5.7.11	La solución debe proveer soporte completo para ACL de depósitos, keys grants de claves, etc.
5.7.12	La solución debe poder realizar una evaluación completa de las cláusulas Permitir vs Denegar.
5.7.13	La solución debe proveer soporte total para Boundaries y SCP.
5.7.14	La solución debe proveer soporte completo para condiciones.
5.7.15	La solución debe proveer soporte completo para Azure RBAC.
5.7.16	La solución debe proveer soporte completo para políticas de claves de acceso, claves de cuentas de almacenamiento y claves de bases de datos.
5.7.17	La solución debe proveer soporte completo para Azure PIM.
5.7.18	La solución debe proveer soporte completo para GCP RBAC.
5.7.19	La solución debe proveer soporte completo para grupos especiales de GCP.

5.7.20	La solución debe proveer visibilidad de identidad de las cargas de trabajos y los derechos otorgados a las cuentas de servicio de Kubernetes.
5.7.21	La solución debe ser capaz de la detección automática de rutas de escalación de privilegios.
5.7.22	La solución debe categorizar los permisos según el riesgo (por ejemplo, acceso administrativo, acceso a datos, escalada de privilegios).
5.7.23	La solución debe detectar el uso efectivo de los derechos otorgados (que puede hacer y acceder).
5.7.24	La solución debe identificar identidades privilegiadas.
5.7.25	la solución debe identificar identidades inactivas.
5.7.26	La solución debe identificar identidades con privilegios excesivos según la actividad (permisos excesivos).
5.7.27	La solución debe proveer recomendaciones automáticas de privilegios mínimos basadas en la actividad.
5.7.28	La solución debe identificar identidades privilegiadas de terceros.
5.7.29	La solución debe identificar la falta de uso de MFA.
5.7.30	La solución debe Identificar credenciales estáticas no utilizadas (e.g., claves de acceso).
5.7.31	La solución debe identificar identidades privilegiadas vinculadas a recursos expuestos.
5.7.32	La solución debe permitir consultar permisos entre organizaciones (e.g., quién tiene un permiso específico sobre recursos, escenarios de separación de funciones, permisos confidenciales, etc.).
5.8	**Privilegios Mínimos**
5.8.1	La solución debe analizar el uso efectivo de los permisos según la actividad, incluido el conocimiento de acciones no registradas y escenarios complejos.
5.8.2	La solución debe detectar y corregir identidades inactivas (humanas, máquinas, usuarios federados).
5.8.3	La solución debe detectar identidades nativas de la nube con permisos excesivos (no utilizados).
5.8.4	La solución debe detectar identidades federadas con permisos excesivos (no utilizados).
5.8.5	La solución debe evaluar el riesgo de permisos excesivos para cada identidad, recurso o alcance de implementación (e.g., cuenta, suscripción).
5.8.6	La solución debe proporcionar recomendaciones con privilegios mínimos para identidades nativas de la nube (incluidos terceros).

5.8.7	La solución debe evaluar los conjuntos de permisos de AWS SSO y su uso.
5.8.8	La solución debe proveer recomendaciones de privilegios mínimos para políticas basadas en recursos.
5.8.9	La solución debe proporcionar recomendaciones con privilegios mínimos para identidades federadas.
5.8.10	La solución debe generar recomendaciones granulares de recursos con privilegios mínimos en un lenguaje nativo de la nube (e.g., JSON, Terraform).
5.8.11	La solución debe ser capaz de corrección automática, en el producto, a través de la API del proveedor de servicios en la nube (CSP) (en 1 clic).
5.9	**Seguridad de Datos**
5.9.1	La solución debe ser capaz de identificar todos los sistemas de almacenamiento de datos en la nube (almacenamiento de objetos, bases de datos, etc.).
5.9.2	La solución debe detectar y proveer un diagrama de los derechos sobre los sistemas de almacenamiento de datos.
5.9.3	La solución debe detectar sistema de almacenamiento de datos público y accesible desde otras entre cuentas/subscripciones/organizaciones.
5.9.4	La solución debe ser capaz de etiquetar los sistemas de almacenamiento de datos confidenciales.
5.9.5	La solución debe limitar el acceso a recursos confidenciales mediante recomendaciones de políticas con privilegios mínimos.
5.9.6	La solución debe detectar malas configuraciones en los sistemas de almacenamiento de datos almacenados (e.g, cifrado, rotación de keys).
5.9.7	La solución debe ser capaz de detectar acceso inusual a datos (detección de anomalías).
5.9.8	La solución debe proveer recomendaciones de privilegios mínimos para la configuración basada en recursos (e.g., políticas de depósito AWS S3).
5.10	**Seguridad de Red**
5.10.11	La solución debe proveer un inventario de activos de recursos y configuraciones de red.
5.10.12	La solución debe proveer detección de configuraciones erróneas de la red (e.g., uso de una versión TLS insegura).

5.10.13	La solución debe detectar recursos computacionales y de datos expuestos públicamente.
5.10.14	La solución debe proveer visibilidad del acceso a la red de haciendo uso otras cuentas / subscripciones / organizaciones.
5.10.15	La solución debe proveer un diagrama de la ruta de acceso de red para los recursos expuestos.
5.10.16	La solución debe diferenciar entre exposición directa e indirecta.
5.10.17	La solución debe diferenciar entre exposición de red amplia y restringida.
5.11	**Protección de Cargas de Trabajo**
5.11.1	La solución debe ser capaz de escanear cargas de trabajo en la nube (e.g. máquinas virtuales, contenedores).
5.11.2	La solución debe ser capaz de detectar vulnerabilidades en máquinas virtuales.
5.11.3	La solución debe ser capaz de detectar vulnerabilidades en imágenes de contenedores.

5.11.4	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad. Dicha calificación deberá ser obtenida a partir de los siguientes factores: - La priorización deberá correlacionar información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación. - El modelo de priorización deberá ser capaz de predecir si una vulnerabilidad tiene posibilidades de explotación en el futuro cercano. - La priorización deberá considerar elementos de evaluación diversos, como: edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, número de días desde que se conoció una actividad de amenaza sobre la vulnerabilidad
5.11.5	La solución debe ser capaz de detectar sistemas operativos sin parches.
5.11.6	La solución debe ser capaz de detectar vulnerabilidades en contenedores y máquinas virtuales con accesos privilegiados.
5.11.7	La solución debe ser capaz de detectar vulnerabilidades máquinas virtuales y contenedores expuestos públicamente.
5.12	**Seguridad de Kubernetes.**
5.12.1	La solución debe proveer soporte completo para clústeres de Kubernetes administrados (GKE, AKS, EKS).
5.12.2	La solución debe proveer un inventario de activos de recursos de Kubernetes.

5.12.3	La solución debe detectar malas configuraciones en Kubernetes.
5.12.4	La solución debe ser capaz de evaluar los entornos de Kubernetes comparándolos con marcos de referencia de seguridad de la industria (e.g., CIS).
5.12.5	La solución debe proveer visibilidad de los usuarios y cuentas de servicio de Kubernetes.
5.12.6	La solución debe proveer visibilidad de permisos otorgado (Kubernetes RBAC).
5.12.7	La solución debe proveer visibilidad de la identidad de la carga de trabajo y los derechos de nube otorgados a las cuentas de servicio de Kubernetes.
5.12.8	La solución debe proveer detección de servicios de Kubernetes expuestos públicamente.
5.13	**Infraestructura como Código (IaC)**
5.13.1	La solución debe generar automáticamente recomendaciones con privilegios mínimos en plantillas Terraform/CloudFormation.
5.13.2	La solución debe integrarse con herramientas de pipeline de CI/CD (por ejemplo, GitHub Actions, Jenkins, Azure Pipelines, Terraform Cloud) para detectar configuraciones incorrectas durante el SDLC.
5.13.3	La solución debe integrarse con repositorios de control de código fuente para detectar configuraciones erróneas existentes en (IaC).
5.13.4	La solución debe ser capaz de escanear los archivos de código y plan de Terraform en busca de configuraciones erróneas.
5.13.5	La solución debe escanear las plantillas de CloudFormation en busca de configuraciones incorrectas.
5.13.6	La solución debe asociar recursos en la nube mal configurados con el código (IaC) para identificar a los propietarios.
5.13.7	La solución debe sugerir correcciones al código para recursos en la nube aprovisionados a partir del código.
5.14	**Flujos de Trabajo y remediación**
5.14.1	La solución debe permitir personalizar los flujos de trabajo y las automatizaciones según el entorno/política/riesgo (e.g, envíe notificaciones por correo electrónico sobre problemas críticos, cree tickets sobre problemas en producción).
5.14.2	La solución debe proveer soporte integrado para la gestión de hallazgos de seguridad (e.g., excluir, resolver, posponer).

5.14.3	Los hallazgos identificados por la solución deben contener pasos de remediación y el contexto completo necesario para resolver el problema subyacente.
5.14.4	La solución debe proveer corrección automática con un solo clic utilizando las API del proveedor de la nube.
5.14.5	La solución debe permitir automatizar los flujos de trabajo a través de API.
5.14.6	La solución debe permitir a los usuarios comentar sobre los hallazgos.
5.14.7	El proceso de priorización de la solución debe ser basado en riesgos evaluando el contexto ambiental completo.
5.15	**Integraciones y Automatizaciones**
5.15.1	La solución debe proveer integración con herramientas de colaboración (e.g. Teams, Slack, e-mail) para el envío de notificaciones.
5.15.2	La solución debe proveer la capacidad de enviar los hallazgos a herramientas tipo SIEM (e.g. Splunk, QRadar, DataDog).
5.15.3	La solución debe permitir reenviar los hallazgos a sistema de tickets (e.g. JIRA, ServiceNow) para gestión de proyectos e ITSM.
5.15.4	La solución debe permitir personalizar los flujos de trabajo mediante activadores de webhooks.
5.16	**API**
5.16.1	La solución debe proveer soporte a GraphQL-based API.
5.16.2	La solución debe proveer control de acceso al API basado en roles (RBAC-based).
5.16.3	La solución debe permitir hacer consultas de datos de la plataforma vía API.
5.17	**Implementación**
5.17.1	La solución debe proveerse como servicio en la nube.
5.17.2	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
5.18	**Soporte**
5.18.1	El fabricante de la herramienta debe proveer soporte 24 x 7 x 365.
5.18.2	Los tiempos de respuesta inicial para problemas críticos debe ser de una hora o menos.

5.18.3	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
5.18.4	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II)
6. SEGURIDAD EN DIRECTORIO ACTIVO	
6.1.	**Generalidades**
6.1.1	Se requiere una solución de auditoría y monitoreo permanente sobre la configuración del directorio activo, con el fin de garantizar autonomía e imparcialidad en la detección de fallas. La cual cuente con una cobertura para 2000 usuarios activos del directorio activo de la entidad por un periodo de 12 meses. Considerando un crecimiento del 10% en caso de ser necesario.
6.1.2	La solución suministrada deberá ser de un fabricante tercero al fabricante del Directorio activo actual a monitorear con el fin de garantizar una auditoria de un tercero con miras al aseguramiento de este.
6.1.3	La solución debe proporcionar un análisis basado en grafos sobre las relaciones que se establecen entre los diferentes objetos que componen el directorio activo (usuarios, recursos, privilegios...).
6.1.4	La solución no debe requerir instalación de software o activaciones de funcionalidades sobre el directorio activo a monitorear.
6.1.5	Con el fin de garantizar la adquisición de una solución tecnológicamente madura, con una visión estratégica de mercado y una ejecución operacional comprobada, el fabricante de la solución ofertada deberá demostrar su liderazgo simultáneo en las evaluaciones más recientes de Gartner y Forrester para las tecnologías relevantes. Específicamente, deberá estar posicionado como 'Líder' en: • Gestión del Riesgo de Vulnerabilidades. • Gestión Unificada de Vulnerabilidades El contratista deberá adjuntar la documentación o evidencia pública que certifique la posición de 'Líder' en ambos informes en su versión más reciente disponible antes de la suscripción del acta de inicio
6.1.6	La solución ofertada deberá hacer parte de una plataforma de administración de exposición cibernética.
6.1.7	El contratista deberá mantener vigente duranta la ejecución del contrato y hasta el vencimiento de la licencia de la solución tecnológica ofertada, el certificado de Partner o distribuidor directo autorizado del fabricante.
6.1.8	El contratista deberá entregar hojas de datos (datasheets) o manuales del fabricante evidenciando cumplimiento de la solución.
6.1.9	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.
6.2	**Acceso Administrativo de la Solución**

6.2.1	Para el acceso administrativo a la plataforma se debe permitir la integración con servidores LDAP, uso de SAML o cuentas creadas internamente.
6.2.2	La solución debe permitir la creación de perfiles para personalizar los datos presentados de acuerdo con el rol de la persona que acceda a la consola de administración.
6.2.3	La solución debe proporcionar un registro de toda la actividad administrativa realizada sobre la consola con fines de auditoría.
6.2.4	La solución debe restringir el acceso a los datos y opciones administrativas por medio de la creación de roles personalizados.
6.3	**Visibilidad de la Solución**
6.3.1	La solución debe permitir ver gráficamente la topología del directorio activo monitoreado.
6.3.2	Se deberán ver gráficamente las relaciones del directorio activo para evaluar movimientos laterales desde activos potencialmente comprometidos.
6.3.3	Se deberá ver la posible ruta de ataque para anticiparse a posibles escalaciones de privilegios que lleguen a un activo determinado.
6.3.4	Se deberá poder visibilizar, monitorear y analizar eventos del directorio activo en tiempo real que potencialmente afecten el directorio activo.
6.3.5	La solución ofertada debe contribuir a la visualización de ruta de ataque para los equipos enfocados a actividades de Red y Blue Team.
6.3.6	Se deberá poder visibilizar posibles rutas que puede tomar un atacante para poner en peligro un activo desde un punto de entrada.
6.3.7	Se deberá poder visibilizar los posibles movimientos laterales en Active Directory desde cualquier activo.
6.3.8	Se deberá poder visibilizar todas las rutas de acceso que potencialmente pueden tomar el control de un recurso.
6.3.9	La solución ofertada debe ser compatible con Azure AD (AAD) para expandir el alcance de las identidades en una organización, sin incurrir en costos adicionales.
6.3.10	La solución deberá soportar análisis con usuario de privilegio en caso de ser requerido.

6.4	**Aseguramiento Preventivo**

6.4.1	La solución debe estar en capacidad de hacer una auditoría en tiempo real sobre el directorio activo, para alertar sobre posibles rutas de ataque y malas prácticas de configuración (detección de más de por lo menos 40 malas prácticas en las políticas de directorio activo). Dentro de los hallazgos que ofrezca la solución se deben tener como mínimo: - Configuración débil del protocolo Netlogon - Certificados digitales asociados a cuentas privilegiadas - Controladores de dominio gestionados por usuarios ilegítimos - Uso de "primary group" - Configuración riesgosa de ADCS - Débiles políticas de credenciales - Delegación de Kerberos riesgosa - Falla de consistencia para "SDProp" - Cuentas privilegiadas ejecutando servicios de kerberos - Uso de algoritmos de cifrado débil en el servicio de PKI de directorio activo - Controladores de dominio falsos
6.4.2	La solución debe proporcionar información detallada sobre cada hallazgo, así como el detalle sobre cómo corregir cada configuración no recomendada.
6.4.3	La solución debe ofrecer la opción de análisis de credenciales garantizando que no se almacena información una vez se deshabilita este servicio.
6.4.4	La plataforma ofertada debe soporta una cuenta señuelo cuyo único propósito es detectar a un atacante que intenta comprometer la red a través de Active Directory.
6.5	**Aseguramiento Reactivo**
6.5.1	La solución debe estar en capacidad de alertar de forma automática cuando se estén desarrollando ataques dirigidos al directorio activo, tales como: - Ataques de enumeración - Golden ticket - Yara Detection (debe permitir personalizar reglas Yara para identificar objetivos de ataque) - Password spraying - Dcsync - Dcshadow - OS Credential Dumping - PetitPotam - Explotación de DnsAdmins - Password guessing - Kerberoasting - Extracción de NTDS, entre otros.

6.5.2	La solución debe registrar en un repositorio independiente al directorio activo, los cambios que se realizan a nivel de configuración sobre el mismo.

6.5.3	La solución debe permitir la generación de alertas sobre comportamientos específicos en el Directorio Activo, definidos por el administrador de la plataforma.
6.6	**Reportería**
6.6.1	La solución debe permitir la creación de dashboard personalizados.
6.6.2	La solución debe presentar de forma gráfica las diferentes rutas de ataque que podrían utilizarse para explotar un recurso puntual del directorio. Debe permitirse parametrizar el origen y destino de cada una de estas rutas de ataque para graficar rutas puntuales.
6.6.3	La solución debe presentar de forma gráfica todos los recursos que podrían verse comprometidos a partir de un objeto puntual en el directorio activo.
6.6.4	La solución debe presentar de manera gráfica las relaciones de confianza que se establecen entre los diferentes dominios, así como enunciar las fallas u oportunidades de mejora en estas configuraciones desde la perspectiva de seguridad.
6.7	**Indicadores de Ataque e Indicadores de Exposición**
6.7.1	La tecnología al tener la capacidad de detectar ataques sobre el directorio activo deberá permitir: - Sobre el incidente detectado explorar la descripción del mismo usando el framework MITRE ATT&CK - Analizar en profundidad los detalles acerca del ataque detectado sobre el AD - Analizar cada amenaza en la línea del tiempo
6.7.2	Deberá poder hacer recomendaciones sobre qué acción tomar acorde a la severidad del Indicador detectado.
6.7.3	La tecnología al tener capacidades de validar la exposición deberá permitir: - Asignar niveles de gravedad al flujo de eventos revisados - Disparar alertas cuando detecta regresiones de seguridad
6.8	**Implementación**
6.8.1	La solución debe proveerse como servicio en la nube o en formato de despliegue en premisa. (Máquinas virtuales o bare metal).
6.8.2	Este servicio no debe requerir la instalación de agentes o software en los controladores de dominio ni la creación de cuentas con privilegios administrativos.
6.8.3	La solución debe estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario común con privilegios de lectura sobre los contenedores de objetos borrados y atributos de credenciales.

6.8.4	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
6.9	**Integraciones y Alertas**
6.9.1	La solución debe generar alertas en formato Syslog o por correo electrónico.
6.9.2	La plataforma debe soportar integración con plataformas de correlación tipo SIEM y SOAR por medio de protocolo Syslog.
6.9.3	La solución ofertada deberá soportar integraciones vía API y las mismas deben estar documentadas.
6.10	**Soporte**
6.10.1	El fabricante de la solución debe proveer soporte 24 x 7 x 365.
6.10.2	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
6.10.3	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
7. GESTIÓN DE ACTUALIZACIONES	
7.1	**Generalidades**
7.1.1	Se requiere una solución de gestión de actualizaciones, con el fin de visibilizar, priorizar y remediar todas las brechas de seguridad sobre la infraestructura. La cual cuente con una cobertura para 2000 activos por un periodo de 12 meses. Esta deberá ser del mismo fabricante de la solución de ciber exposición u OEM de fábrica.
7.1.2	La solución debe optimiza el ancho de banda de la red mediante el uso de tecnología peer-to-peer (P2P), que distribuye parches de manera eficiente sin limitar el ancho de banda. Esto garantiza que los parches se entreguen rápidamente sin interferir con otras operaciones comerciales críticas. Además, admite la entrega fuera de la red, lo que garantiza que los puntos finales reciban parches independientemente de su estado de conexión.
7.1.3	La solución debe prioriza la protección y la optimización del rendimiento de la red. Los enlaces WAN están protegidos de la saturación mediante funciones que controlan el flujo de entrega de contenido, como la recolección predictiva de ancho de banda, que monitorea el tráfico en la WAN y libera ancho de banda para otro tráfico comercial según sea necesario y luego recolecta el ancho de banda no utilizado a medida que se completa otro tráfico.
7.1.4	La solución debe incluir un sistema de aprobación sólido que se puede utilizar como parte de su estrategia de automatización. Puede asignar grupos de partes interesadas a las responsabilidades de aprobación para cada estrategia de parches que cree. Las aprobaciones se pueden adaptar a sus requisitos únicos, lo que le permite definir aprobaciones de varios niveles.

7.1.5	La solución debe permitir implementaciones por fases, con el fin de permitir la prueba de parches en un pequeño grupo de dispositivos específicos antes de pasar a grupos de distribución cada vez más grandes para cubrir su entorno de producción.
7.1.6	La solución debe automatizar todo el proceso de implementación de parches en sus terminales. Cuando el equipo de metadatos lanza un nuevo parche, el servidor del cliente descargará los metadatos en 5 minutos y los distribuirá a la red para identificar los dispositivos que requieren el nuevo parche.
7.1.7	La solución debe utilizar un sistema peer-to-peer exclusivo de clase empresarial que optimiza la distribución de contenido a través de redes complejas, aprovechando el hardware existente de los puntos finales para participar en el almacenamiento en caché y la transferencia de contenido a todos los dispositivos. Junto con nuestros protocolos de optimización de red, este sistema puede escalar a cientos de miles de puntos finales sin afectar la red ni a los usuarios.
7.1.8	La solución debe utilizar reglas de aplicación de parches u objetos de intención que usted crea para identificar grupos de dispositivos, implementaciones por niveles, personalizaciones de instalación, cronogramas y colas, ventanas de mantenimiento estáticas o dinámicas, entre otros.
7.1.9	La solución debe estar basado en agentes los cuales permite la distribución instantánea de políticas a los clientes para que puedan procesar los parches necesarios de manera rápida y eficiente.
7.1.10	La solución debe utilizar una consola para la gestión de vulnerabilidades y una para la gestión de parches independientes, entre las cuales intercambien información de riesgos y probabilidades de explotación de brechas.
8. CONECTORES DE TERCEROS	
8	**Generalidades**
8.1.1	La solución deberá ser parte de una plataforma de gestión de exposición.
8.1.2	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).
8.1.3	La solución deberá integrar datos de riesgo y vulnerabilidades de toda la entidad.

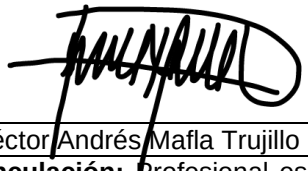
8.1.4	La solución deberá integrar plataformas de al menos las siguientes categorías: - Seguridad de Aplicaciones - Nube - Evaluación de Vulnerabilidades - Colaboración - Inteligencia de Amenaza - Bug Bounty - Inventario de Activos - Deloyment - Seguridad de Endpoint - Inteligencia de Remediación - IoT
8.1.5	La solución debe permitir Tableros de control y exportaciones automatizados.
8.1.6	La solución debe permitir Información de exposición unificada permitiendo Múltiples tableros de control diseñados previamente para CISO y profesionales a lo largo de todos los activos y hallazgos.
8.1.7	La solución debe permitir Tableros de control personalizados.
9. EXPOSICIÓN DE DOMINIOS E IDENTIFICACIÓN DE CREDENCIALES EXPUESTAS	
9.1	**Generalidades**
9.1.1	Se requiere solución para exposición de dominios e identificación de credenciales expuestas, para 5 dominios, por un periodo de 12 meses.
9.1.2	La solución debe tener cobertura 360° de datos expuestos en fuentes externas, incluyendo como mínimo dominios, subdominios, direcciones IP públicas, buckets de almacenamiento, repositorios de código y menciones en comunidades clandestinas.
9.1.3	La solución debe contar con protección de datos sensibles, mediante cifrado en reposo con estándar AES-256 y en tránsito con TLS 1.3. garantizando su confidencialidad.
9.1.4	La plataforma de la solución debe estar disponible en inglés y español (UI, reportes, documentación y soporte técnico).
9.2	**Funcionalidades**
9.2.1	La solución debe contar con detección de credenciales expuestas y data leaks, que permita identificar cuentas y contraseñas en texto plano o cifradas, con asignación de niveles de riesgo mediante inteligencia artificial.
9.2.2	La solución debe tener plataforma de gestión de incidentes, que permita centralizar hallazgos, definir su ciclo de vida (abierto, en progreso, resuelto, ignorado) y gestionar flujos de remediación con métricas de cumplimiento y reportes ejecutivos.

9.2.3	La solución debe contar con motor de scoring configurable, que permita asignar niveles de severidad a incidentes y hallazgos entre 0 y 100 según criterios ajustables.
9.2.4	La plataforma debe dar registro histórico de cambios y auditoría, que permita visualizar quién realizó modificaciones sobre activos e incidentes, con fecha y detalle.
9.2.5	La solución debe dar definición y gestión de SLA para incidentes de ciber exposición, permitiendo controlar tiempos máximos de resolución y medir métricas como MTTR (Mean Time To Resolve).
9.2.6	La solución debe permitir creación de reportes ejecutivos en formato PDF, o json para integrar en otras plataformas.
9.2.7	La plataforma debe dar actualización diaria de nuevas fuentes Deep/Dark Web y feeds OSINT, para mantener vigente la cobertura de vigilancia.
9.2.8	La plataforma debe tener enriquecimiento contextual de los hallazgos, incorporando información mínima como fecha de detección, fuente de origen, usuario que publica, categoría del hallazgo y su relevancia.
9.2.9	La solución debe contar con la incorporación de inteligencia de amenazas proveniente de fuentes Deep y Dark Web, incluyendo foros, mercados clandestinos, canales de mensajería y paste-sites, para detección temprana de filtraciones o menciones de activos críticos.
9.2.10	La plataforma debe contar con panel de tendencias mensuales, que visualice patrones de comportamiento de ciber exposición, incluyendo picos de actividad y comparativas porcentuales.
9.2.11	La solución debe tener funcionalidad de búsquedas ad-hoc, para localizar filtraciones, correos electrónicos, dominios o palabras clave específicas en las fuentes monitoreadas.
9.2.12	La solución debe clasificar y priorizar los activos monitoreados según su valor para el negocio, permitiendo gestiónar de forma diferenciada los activos críticos.
9.2.13	La plataforma debe contar con visualización de histogramas de filtraciones por mes, así como ranking de usuarios, dominios o URLs más afectados.
9.2.14	La solución debe contar con módulo de análisis de tendencias, con generación de gráficas interactivas exportables a formatos PNG.
9.2.15	La plataforma debe permitir exportar datos a CSV y JSON desde cualquier vista (credenciales, inteligencia, incidentes).
9.2.16	La solución debe ser modo multi-tenant para MSSP / grupos empresariales (segregación por tenant).
9.2.17	La fábrica debe contar con un monitoreo continuo de filtración de datos de 5 dominios.

9.2.18	La solución debe tener capacidad de Take Down, mediante créditos, los cuales sólo pueden ser consumidos hasta que el Take Down sea efectivo, esto debe estar soportado por el datasheet del fabricante.
9.2.19	El fabricante de la tecnología de exposición de dominios deberá ser diferente a la del firewall y WAF de la Entidad.
9.3	**Alertas**
9.3.1	La solución debe contar con notificaciones automáticas mediante plantillas predefinidas, dirigidas a usuarios internos o externos, informando sobre hallazgos de exposición o compromisos detectados.
9.4	**Implementación**
9.4.1	La solución debe proveerse como servicio en la nube.
9.4.2	A la suscripción del acta de inicio se deberán adjuntar la hoja de vida del personal mínimo requerido en la presente ficha técnica, incluyendo la del líder de implementación.
9.4.3	La solución deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
9.5	**Soporte**
9.5.1	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
9.5.2	Proporcionar portal de soporte 24×7.
9.5.3	El fabricante debe contar con tiempos de respuesta < 4 h críticos.
10. SERVICIOS DE IMPLEMENTACION, SOPORTE Y REMEDIACION	
10.1	**Generalidades**
10.1.1	Se requiere que el proveedor de la solución realice la totalidad de la implementación de las soluciones indicadas en la ficha técnica. Aplicando las mejores prácticas del fabricante y realizando la configuración de las plataformas que se requieran acorde a las condiciones solicitadas por el IDU en la fase de diseño del servicio.
10.1.2	Se requiere que el proveedor de la solución realice el soporte de las tecnologías consideradas en un esquema 7 x 24 x 365 con personal dedicado para recepción de casos, solución de fallos y escalamiento de problemáticas de funcionamiento al fabricante. Este servicio deberá tener las capacidades de recepción de casos, seguimiento a los mismos y tracking a la solución de las problemáticas que se presenten. Se aclara que el IDU siempre contara con el soporte de fabricante durante la duración del servicio; esto para que sea usado por el proveedor como apoyo para la solución de problemáticas de las plataformas

10.1.3	Se requiere que el proveedor preste el soporte de la plataforma en un esquema 7 x 24 x 365 el cual apoye con la realización de configuraciones, seguimiento a issues, escalamiento de casos y actividades de remediación asociadas a la gestión en las diferentes capacidades de la solución ofertada. Se aclara que el contratista deberá hacer seguimiento a las remediaciones, recomendación en soluciones extraídas de la herramienta, apoyo en la investigación inicial de los riesgos encontrados y escalamiento a las áreas del IDU para que estos sean aplicados y ejecutados por los especialistas y administradores de las plataformas del IDU. El IDU entregará accesos al sistema de atención de usuarios para que se pueda vincular este servicio a los flujos de soporte y así lograr la creación de casos para la realización de seguimientos en las áreas responsables de la aplicación. Sin embargo, en el caso de las capacidades de gestión de actualizaciones de la tecnología se requiere que el soporte permita la correcta configuración de la herramienta para que los procesos internos del IDU se cumplan y se logren las actualizaciones que la herramienta permita de forma automatizada.
10.1.4	El Contratista deberá contar con personal que preste los servicios de Implementación, Soporte y Remediación, para lo cual se deberán presentar las respectivas hojas de vida del personal requerido a la suscripción del acta de inicio.
10.1.5	Todo el servicio deberá estar enmarcado en las mejores prácticas del PMBOK, contando con un gerente de proyecto para la prestación del servicio hasta el cierre del proyecto.
10.1.6	Se requiere realizar una transferencia de conocimientos por parte de un experto en IA, de 4 horas en buenas prácticas de manejo de Agentes de IA aplicados a la ciberseguridad; de tal forma que se pueda tener conocimiento de cómo hacer un mejor uso de este tipo de motores en tecnologías de fabricantes de mercado.
10.2	**Gerente de Proyecto**
10.2.1	Título profesional en Ingeniería de Sistemas / Ingeniería electrónica / Ingeniería de Software / Ingeniería de Telecomunicaciones según NBC del SNIES.
10.2.2	Especialización o Maestría en Gerencia de Proyectos informáticos o Gerencia de Proyectos en Telecomunicaciones
10.2.3	Deberá contar con: Certificaciones en CISSP o CISM
10.2.4	Experiencia general mínima de diez (10) años contados a partir de la obtención del título profesional.
10.2.5	Experiencia específica mínima de cinco (05) años en gestión de proyectos de ciberseguridad y/o y/o seguridad digital y/o seguridad de la información
10.2.6	**Líder de implementación**
10.2.7	Título profesional en Ingeniería de Sistemas / Ingeniería Informática / Ingeniería electrónica / Ingeniería de Software / Ingeniería de Telecomunicaciones según NBC del SNIES
10.2.8	Especialización o Maestría en Seguridad Informática o Seguridad de las tecnologías de la información.

10.2.9	Deberá contar con: Certificación como Auditor Interno o líder ISO 27001:2022 o CEH o CTIA
10.2.10	Experiencia general mínima de diez (10) años contados a partir de la obtención del título profesional
10.2.11	Experiencia específica mínima de cinco (5) años como Implementador de proyectos de ciberseguridad y/o seguridad digital y/o seguridad de la informaciónen empresas públicas o privadas.
10.3	**Gestor de Remediación**
10.3.1	Título profesional en Ingeniería de Sistemas / Ingeniería Informática / Ingeniería electrónica / Ingeniería de Software / Ingeniería de Telecomunicaciones según NBC del SNIES
10.3.2	Especialización o Maestría en Seguridad Informática
10.3.3	Deberá contar con: Certificación como Auditor Interno o líder ISO 27001:2022 o CEH o CTIA.
10.3.4	Experiencia general mínima de cinco (5) años contados a partir de la obtención del título profesional.
10.3.5	Experiencia específica mínima de tres (3) años como Líder o coordinador o gestor de proyectos de ciberseguridad.
10.3.6	El Gestor de remediación se requiere en un horario 7x24x365 de forma remota o en sitio durante 12 meses.

Elaborado por:	**Avalado por:**
Firma: 	**Firma** 
Nombre: Héctor Andrés Mafla Trujillo	**Nombre:** José Alfredo Ruíz Peralta
Cargo o vinculación: Profesional especializado – STRT.	**Cargo o vinculación:** Subdirector Técnico de Recursos Tecnológicos