BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA

SECCIÓN DE COMPRA Y CONTRATACIONES

FICHA TECNICA

12 de diciembre, 2022

NO. SOLICITUD:	**BAGRICOLA-CCC-LPN-2022-0006**	**OBJETO DE LA COMPRA:**	**CONTRATACION DE LA CONSULTORIA Y ADQUISICION DE UNA SOLUCIÓN DE PREVENCIÓN FUGA DE INFORMACIÓN (DLP)**
RUBRO:	81111801 - Seguridad de computadores, redes o Internet	**PLANIFICADA:**	Si

DETALLES, ESPECIFICACIONES Y CONDICIONES ESPECIALES DE LOS SERVICIOS A SER OFERTADOS

1. CONSULTORÍA TRATAMIENTO INTERNO DE INFORMACIÓN		
No.	**CONSULTORÍA Y ACOMPAÑAMIENTO**	**CUMPLE/ NO CUMPLE**
1.1	El oferente debe preparar un cronograma de actividades con tareas y responsables para realizar un levantamiento de las políticas, procedimientos e informaciones internas, medir la madurez actual del Banco, respecto a la detección, protección, clasificación y etiquetado de la información en tránsito y almacenada del Banco.	
1.2	El oferente debe identificar junto con el personal de Seguridad de Información del Banco, los responsables y dueños de las informaciones. Se deberá crear un inventario de dueños (owner) de las informaciones.	
1.3	El oferente debe revisar y validar la documentación existente y faltante (política, procedimiento, matrices, otros), relacionados con la identificación, etiquetado, clasificación, detección y prevención de fuga de información.	
1.4	El oferente debe brindar una guía y asesoría sobre la documentación faltante o carente de directrices (política, procedimiento, matrices, otros), relacionados con la identificación, etiquetado, clasificación, detección y prevención de fuga de información.	
1.5	El oferente debe impartir una capacitación-charla para educar y concientizar a los responsables y dueños (owners) de las informaciones, sobre el uso, etiquetado, clasificación, detección y protección de las informaciones.	
1.6	El oferente debe impartir una charla para educar y concientizar a los miembros del Directorio Ejecutivo, Directores y Gerentes del Banco, sobre la importancia y prevención del uso y manejo de las informaciones del Banco.	
2. MÓDULO DETECCIÓN Y PREVENCIÓN FUGA DE INFORMACIÓN		
No.	**ARQUITECTURA Y GESTION**	**CUMPLE/ NO CUMPLE**
2.1	La solución debe proporcionar un marco de políticas único en todos los canales de exfiltración de datos (p. ej., correo electrónico, web, aplicación en la nube, impresión, aplicación de punto final, medios extraíbles, uso compartido de archivos)	
2.2	Todas las funciones de gestión, incluidos los cambios de configuración y las actualizaciones, deben realizarse desde una consola central	
2.3	El sistema debe admitir el acceso basado en roles y la administración delegada con roles predefinidos y personalizables: Auditor: administre políticas, reglas y clasificadores para el cumplimiento normativo. Administrador de incidentes: acceso a informes, detalles de incidentes y flujo de trabajo. Capacidad para gestionar incidencias. Policy Manager - Acceso a todos los incidentes. Capacidad para calificar y asignar incidentes. Superadministrador: permiso completo de acceso, administración y configuración. Administrador del sistema: acceso personalizable a las tareas administrativas.	

2.4	La solución propuesta debe admitir la integración con Active Directory o File Directory (CSV)	
2.5	La solución debe admitir la creación/excepción de políticas en función del directorio de usuario/grupo, máquina, red, dominio	
2.6	La solución debe tener la capacidad de auditar los cambios (p. ej., iniciar/cerrar sesión, cambios de reglas, registros del sistema, registros de tráfico)	
2.7	Capacidad para que el sistema notifique cuando tiene problemas de conexión	
2.8	Capacidad de integración (a través de syslog o extracción de base de datos) con SIEM para fines de registro y alerta	
2.9	La solución debe proporcionar escalabilidad futura para todos los componentes de dlp (correo electrónico, web, rastreadores, endpoint)	
2.10	La solución debe admitir entornos de infraestructura virtualizada, como Azure o AWS para el portal de administración, la base de datos y otros componentes.	
2.11	La solución debe tener integración nativa con clasificaciones de datos (Boldon James, Microsoft AIP, Seclore, Titus).	
2.12	La solución propuesta debe poder implementar el agente utilizando métodos comunes de implementación de software como GPO, SCCM, JAMF, etc.	
2.13	La solución debe brindar la capacidad de verificar el estado del agente y también informar sobre cualquier agente que no esté funcionando correctamente.	
2.14	Cualquier punto de integración debe estar encriptado, a través de https (entrante/saliente)	
2.15	La solución debe ser compatible con Microsoft RMS	
2.16	La solución debe usar una base de datos relacional empresarial, como SQL	
2.17	La arquitectura de la solución debe admitir sitios remotos y usuarios de red distribuidos en muchas ubicaciones diferentes. Describa cualquier limitación en cuanto al número de componentes. Describa una implementación típica y dónde reside cada componente. Adjunte un diagrama de arquitectura detallado.	
2.18	La solución debe ser compatible con la autenticación de dos factores para el acceso del administrador a la consola de gestión	
2.19	Debe tener la capacidad de integrarse con Active Directory o LDAP, para obtener detalles e información adicional de los usuarios involucrados en un incidente detectado.	
2.20	Debe tener compatibilidad para la instalación, al menos, en los siguientes sistemas operativos: - Microsoft Windows Server 2012 R2 o superior. - Red Hat Enterprise Linux 7.5 o superior.	
No.	**CAPACIDAD DE SEGURIDAD EN DATOS Y DETECCIÓN DE DATOS**	**CUMPLE/ NO CUMPLE**
2.21	La solución debe tener políticas específicas de cumplimiento listas para usar basadas en la región y el tipo de industria.	
2.22	La solución debe tener políticas predefinidas (más de 1500) basadas en RegEX, diccionarios o secuencias de comandos y debe poder seleccionar políticas según la correlación del país y las industrias.	

2.23	La solución debe proporcionar políticas predefinidas para identificar posibles expresiones que sean indicativas de acoso cibernético, patrones autodestructivos o descontento de los empleados.	
2.24	La solución debe tener políticas de indicadores de riesgo de robo de datos (por ejemplo, datos enviados durante horas inusuales, correo electrónico a competidores, comunicación sospechosa de malware, currículums, etc.)	
2.25	La solución debe tener la capacidad de usar una sola política para escanear datos donde sea que se almacenen, transmitan o usen, tanto en la red como en el punto final. Además, los canales de destino se pueden modificar fácilmente para cualquier política. (Ej: si desea ampliar la cobertura de una política aplicada para SMTP para incluir también HTTP y HTTPS.	
2.26	Las excepciones basadas en reglas deben ser simples de diseñar e implementar para reducir los falsos positivos.	
2.27	La solución debe permitir una sintaxis flexible para vincular datos a aplicaciones específicas, servidores de archivos, redes compartidas, impresoras y patrones de contenido únicos	
2.28	La solución debe admitir tipos de archivos verdaderos predefinidos	
2.29	La solución debe admitir condiciones de políticas basadas en lógica booleana (Y, O, NO)	
2.30	La solución debe admitir datos confidenciales en diferentes idiomas. Para los idiomas no admitidos, describa el comportamiento esperado del proceso de detección.	
2.31	La solución debe extraer e inspeccionar el contenido basado en texto de archivos y archivos adjuntos	
2.32	La solución debe analizar los metadatos del archivo	
2.33	La solución debe admitir huellas dactilares de archivos parciales y hash completos para todos los canales de exfiltración de datos	
2.34	La solución debe distinguir entre diferentes tipos de PII o PHI. Ej.: Distinguir entre el número de seguro social de nueve dígitos de un cliente y un número de teléfono de nueve dígitos sin la presencia de una palabra clave (por ejemplo, "SSN").	
2.35	La solución debe ser compatible con la inspección de tipos de archivos (ZIP, TAR) para detectar contenido con huellas dactilares.	
2.36	La solución debe admitir el análisis de archivos y archivos adjuntos de gran tamaño (20 MB y más) durante el proceso de contenido con huellas dactilares.	
2.37	La solución debe proporcionar un método para tomar las huellas dactilares de los datos, como los registros de los clientes (datos estructurados)	
2.38	La solución debe proteger al menos 10 millones de filas de contenido específico de una base de datos de información confidencial sin depender de palabras clave o patrones	
2.39	La solución debe admitir un método de detección de aprendizaje automático para códigos fuente, formularios.	
2.40	La solución debe admitir reglas totalmente personalizables con expresiones regulares, palabras clave, frases clave y diccionarios	
2.41	La solución debe ser compatible con el contenido de la lista blanca para eliminar de forma segura la detección de contenido textual	

2.42	La solución debe admitir la detección de varias palabras clave en función de un peso específico	
2.43	La solución debe admitir al menos 5000 listas de palabras clave únicas	
2.44	La solución debe admitir la coincidencia de patrones combinada con la validación. Por ejemplo, detectar patrones comunes de números de tarjetas de crédito y realizar la validación de la suma de verificación para garantizar un número de tarjeta de crédito válido (la verificación "Luhn")	
2.45	La solución debe detectar formatos de archivos cifrados conocidos y desconocidos	
2.46	La solución debe identificar etiquetas de etiquetas de metadatos de Boldon James, Azure Information Protection u otras soluciones de clasificación de datos	
2.47	"Debe tener modelos nativos de políticas de detección basados en regulaciones y mejores prácticas de mercado, para al menos: - GDPR. - HIPAA. - PCI. - SOX	
2.48	Debe tener la capacidad de analizar el contenido en diversos tipos de archivos, al menos para: - CAD (DWG, DXF, VSD). - Comprimidos (ZIP, RAR, GZ, LHA, TAR). - Hojas de cálculo (XLS, XLSX, 123). - Presentaciones (PPT, PPTX). - Texto (TXT, ASCII, HTML, DOC, DOCX). - Otros (PDF, MPP, PUB).	
2.49	Debe tener la capacidad de crear un nuevo formato de archivo "TrueType", basado en su encabezado, para agregar detección de un tipo archivo que no esté previamente soportado en la herramienta.	
2.50	Debe detectar el archivo por su contenido real, y no únicamente por la extensión del archivo.	
2.52	Debe tener la capacidad nativa de detectar números de identificación personal o identificadores de impuestos para al menos cada uno de los siguientes países:- Alemania.- Argentina.- Brasil.- Chile- Colombia.- España.- Estados Unidos.- México.- Reino Unido.	
2.53	Debe permitir detectar rangos de números válidos para ciertos tipos de datos, por ejemplo, un número de tarjeta de crédito válido.	
2.54	Debe permitir el uso de expresiones regulares para la identificación de información sensible.	
2.55	Debe tener la capacidad de detectar la presencia de contenido cifrado y generar un incidente.	
2.56	Debe analizar los protocolos de red más comunes y debe poder bloquear la transferencia de información sensible en al menos: 6.4.1.Web (HTTP / HTTPS). 6.4.2.Correo electrónico (SMTP / POP). 6.4.3.Transferencia de archivos (FTP). 6.4.4.Mensajería instantánea.	

2.57	Debe bloquear y eliminar contenido sensible en las transmisiones de protocolo HTTP/HTTPS y FTP integrándose, al menos los siguientes proxies: - Blue Coat ProxySG. - Cisco IronPort y WSA - Fortinet Fortigate. - Squid Web Proxy. - Websense	
2.58	Debe comprobar si hay contenido confidencial en al menos los siguientes sistemas de archivos: - Sistemas de archivos compatibles con CIFS. - NFS. - SMB	
2.59	Debe analizar el contenido almacenado en entornos complejos, al menos para: - Documentum. - Lotus Notes. - Microsoft Exchange. - Microsoft Sharepoint. - Microsoft SQL Server.	
2.60	Debe supervisar y poder bloquear los intentos de copiar contenido confidencial en el disco duro local (indicar si aplica para Windows, macOS o ambos).	
2.61	Debe permitir monitorear y bloquear la transmisión de información sensible vía navegación HTTP (indicar si aplica para Windows, macOS o ambos).	
2.62	Debe permitir monitorear y bloquear la transmisión de información sensible vía HTTPS, integrándose al menos con los siguientes navegadores (indicar si aplica para Windows, macOS o ambos): - Chrome. - Edge. - Firefox. - Internet Explorer. - Safari.	
2.63	Debe brindar monitoreo y opción de bloqueo de transmisión de información sensible a través de aplicaciones de sincronización de archivos en nube, al menos para los siguientes servicios (indicar si aplica para Windows, macOS o ambos):- Box.- DropBox.- Google Drive.- Microsoft OneDrive.	
2.64	Debe tener la capacidad de bloquear la captura de la pantalla en endpoints Windows (cuando el usuario utiliza la tecla print screen).	
2.65	Debe tener la capacidad de monitorear y prevenir la transferencia de datos confidenciales en endpoints Windows a través de RDP (Remote Desktop Protocol) y LanMan (LAN Manager).	

No.	CAPACIDAD SEGURIDAD DE DATOS EN MOVIMIENTO, EN USO Y EN REPOSO	CUMPLE/ NO CUMPLE
2.66	La solución debe ser compatible con MacOS y WindowOS	
2.67	La solución debe ser compatible con VMWare Horizon y Citrix XenApp	
2.68	La solución debe brindar protección continua de los datos confidenciales, independientemente de si el usuario está dentro o fuera de la red. La "Última política aplicada" siempre debe ser la predeterminada	
2.69	La solución debe detectar los intentos de los usuarios de enviar datos confidenciales por correo electrónico y Web (HTTP/S)	
2.70	La solución debe evitar que los usuarios envíen datos confidenciales mediante cualquier aplicación en la computadora de punto final sin necesidad de abrir una solicitud de función para admitir nuevas aplicaciones.	
2.71	La solución debe evitar la filtración de datos a través de medios extraíbles (por ejemplo, unidades USB)	
2.72	La solución debe poder aplicar diferentes políticas incluso cuando los usuarios usan el mismo punto final	
2.73	Las tareas de descubrimiento de datos de puntos finales deben tener una opción de programador por: una vez, diaria, semanal o continuamente	
2.74	La tarea de descubrimiento de datos de punto final debe tener configuraciones flexibles para escanear solo cuando la computadora está inactiva o pausar el escaneo mientras la computadora está funcionando con baterías	
2.75	La tarea de descubrimiento de datos de punto final debe admitir la inclusión y exclusión por tipo de archivo, carpetas, edad o tamaño	
2.76	La tarea de descubrimiento de datos de punto final debe admitir opciones de escaneo diferencial y completo	
2.77	El descubrimiento de datos de punto final debe tener una opción para preservar el tiempo de acceso original	
2.78	El punto final debe aprovechar las etiquetas de metadatos AIP o Boldon James para imponer la clasificación o reclasificar cuando un archivo infringe una política de datos en reposo.	
2.79	El agente debe ser autorreparable y resistente a manipulaciones.	
2.80	Supervise el portapapeles del endpoint y tome medidas en función de los datos copiados.	
2.81	El agente debe ofrecer un mensaje emergente que puede contener palabrería personalizada cuando el usuario intenta infringir la política.	
2.82	El mensaje emergente debe brindar la oportunidad de proporcionar una justificación comercial cuando una política permite esa acción. La justificación del usuario tiene que ser registrada/registrada en un método que pueda ser leído por otros sistemas	
2.83	Los archivos copiados en dispositivos extraíbles deben cifrarse y los contenidos solo se pueden leer en activos propiedad de la empresa.	
2.84	El punto final debe admitir la visibilidad de los datos copiados en dispositivos de medios extraíbles específicos	
2.85	El punto final debe admitir el cifrado de nivel de administrador y la contraseña de autocifrado del usuario cuando los archivos se copian en medios extraíbles	

2.86	El agente de punto final debe tener un impacto mínimo o nulo en el rendimiento de la máquina.	
2.87	El punto final debe admitir políticas jerárquicas de usuarios/grupos con remediación/respuestas configurables.	
2.88	El punto final de DLP debe ser compatible con los navegadores Edge Chromium, Firefox, Safari (Apple) y Chrome	
2.89	El punto final de DLP debe admitir la supervisión y el bloqueo de datos confidenciales cargados en aplicaciones en la nube y almacenamiento en la nube no autorizados.	
2.90	El punto final de DLP debe admitir un proceso para deshabilitar el agente de punto final con autorización	
2.91	El punto final de DLP debe admitir la capacidad de confiar en la aplicación sin ser supervisado por el agente	
2.92	Debe identificar el movimiento de fragmentos de información confidencial en diferentes tipos de documentos, considerando al menos los siguientes: - Archivos de editor de texto (*.doc y *.docx). - Archivos de hoja de cálculo (*.xls y *.xlsx). - Archivos de presentaciones (*.ppt y *.pptx).	
2.93	El punto final debe admitir las siguientes operaciones en datos confidenciales que su punto final DLP puede abordar: • Controles de copiar y pegar (es decir, actividades del portapapeles) • Control de impresión en impresoras locales o de red • Guardar contenido en diferentes ubicaciones, incluido el almacenamiento en: - Carpetas locales - Recursos compartidos de archivos remotos - Unidades extraíbles conectadas a un sistema de punto final, como unidades USB - Almacenamiento en ubicaciones de almacenamiento en la nube	
No.	**CAPACIDAD DE SEGURIDAD EN DATOS Y DETECCIÓN DE DATOS**	**CUMPLE/ NO CUMPLE**
2.94	La solución debe integrarse con la puerta de enlace SMTP empresarial o puede colocarse entre una puerta de enlace SMTP empresarial para realizar análisis DLP	
2.95	La solución debe ser compatible con Exchange Online (local, híbrido u Office 365)	
2.96	La solución debe tener la capacidad de implementar puertas de enlace SMTP en Azure para poder integrarse fácilmente con O365	
2.97	La solución debe admitir la cuarentena de correo electrónico para los correos electrónicos que violaron las políticas de DLP	
2.98	La solución debe tener cifrado nativo o al menos integrarse con herramientas de cifrado de terceros a través de X-Headers	
2.99	La solución debe admitir archivos adjuntos de más de 25 MB para el análisis DLP	
2.100	Debe permitir bloquear, redirigir y poner en cuarentena condicionalmente los mensajes SMTP en función del contenido del mensaje	

2.101	Debe tener la capacidad de identificar correctamente los mensajes en modo de "copia oculta" (bcc) en un mensaje de correo electrónico generado en el servicio de correo en nube de un tercero, con la capacidad de validar la fuga de datos confidenciales, generando un solo evento por incidente detectado, independientemente del número de destinatarios enumerados en una copia oculta.	
2.102	La solución debe ser compatible con la cuarentena, el cifrado, la eliminación de archivos adjuntos y el permiso para acciones de remediación de correo electrónico	
2.103	La solución debe ser compatible con el análisis de reconocimiento óptico de caracteres (OCR) basado en las políticas DLP creadas	
2.104	Debe ofrecer integración a la infraestructura en la nube que el mismo fabricante de la solución proporciona para el análisis del correo electrónico (malware, phishing y spam) y que brinde capacidad y posibilidad de bloquear o cifrar los correos salientes con información sensible.	
No.	**CAPACIDAD SEGURIDAD DE DATOS EN MOVIMIENTO - ENTORNO WEB**	**CUMPLE/ NO CUMPLE**
2.105	La solución proporciona la capacidad de evitar la fuga de datos a través del canal SSL cuando se integra con su propia puerta de enlace sin necesidad de una solución de terceros ni dependencia del protocolo ICAP	
2.106	La solución debe monitorear múltiples tipos de tráfico web: correo web, publicación web y otros protocolos que usan HTTP/S	
2.107	La solución debe monitorear el tráfico FTP activo y pasivo	
2.108	La solución debe ser compatible con las opciones de implementación de terminales virtualizados	
2.109	La solución debe tener la capacidad de aplicar políticas DLP basadas en categorías web (solo con Forcepoint Web Security)	
2.110	La solución debe bloquear y permitir acciones de remediación web	
2.111	La solución debe ser compatible con la apertura por error o el bloqueo por error cuando se produce un error inesperado	
2.112	La solución debe admitir páginas de bloqueo personalizables	
2.113	La solución debe tener la capacidad de monitorear puertos/protocolos adicionales además de HTTP/HTTP	
2.114	La solución debe tener Secure ICAP nativo para la integración de Proxy, NGFW o CASB	
2.115	La solución debe ser compatible con la integración con otros servidores proxy a través de ICAP o el encadenamiento de servidores proxy.	
2.116	La solución debe ser compatible con la implementación de Azure	
2.117	La solución debe ser compatible con el análisis de reconocimiento óptico de caracteres (OCR) basado en las políticas DLP creadas	
No.	**CAPACIDAD DE RED**	**CUMPLE/ NO CUMPLE**
2.118	La solución debe ser compatible con el modo de conexión SPAN/Mirror Port	
2.119	La solución debe ser compatible con VLAN	
2.120	La solución debe admitir la inclusión de redes específicas	

2.121	La solución debe admitir la inclusión de servicios específicos (HTTP, correo electrónico, FTP) y puertos	
2.122	La solución debe ser compatible con el análisis OCR basado en las políticas DLP creadas	
No.	**CAPACIDAD EN LA NUBE**	**CUMPLE/ NO CUMPLE**
2.123	La solución debe aprovechar el mismo marco de políticas de otros canales de DLP para los canales DLP Cloud API y DLP Cloud Proxy (en línea).	
2.124	La solución debe tener integración API con las principales aplicaciones en la nube: Office365, G-Suite, Box, Dropbox, Salesforce y ServiceNow	
2.125	La solución debe ser compatible con el análisis de las actividades de carga, descarga y uso compartido de aplicaciones en la nube para identificar cualquier posible infracción de DLP.	
2.126	La solución debe admitir las siguientes acciones de remediación para el análisis de actividades de la API: poner en cuarentena con nota personalizable, poner en cuarentena sin nota, dejar de compartir externo, dejar de compartir interno, dejar de compartir todo y solo auditar	
2.127	La solución debe poder monitorear/controlar las actividades de carga/descarga de la aplicación en la nube que violan las políticas de DLP desde dispositivos administrados y no administrados	
2.128	La solución debe tener granularidad para aplicar políticas solo para aplicaciones en la nube específicas según la operación del usuario (por ejemplo, cargar/adjuntar/descargar archivos)	
2.129	La solución debe admitir el escaneo de datos en reposo a través de una conexión API para Office365, G-Suite, Box, Dropbox, SalesForce y ServiceNow	
2.130	La solución debe admitir acciones de remediación para el análisis de datos en reposo cuando los archivos violan las políticas de DLP	
2.131	La solución debe admitir las siguientes acciones de remediación para el análisis de datos en reposo: poner en cuarentena con nota personalizable, poner en cuarentena sin nota, dejar de compartir externo, dejar de compartir interno, dejar de compartir todo y solo auditar	
2.132	Capacidad para aplicar políticas granulares basadas en la actividad del usuario de la aplicación en la nube (API sin conexión): carga de archivos, descarga de archivos, uso compartido externo de archivos, uso compartido de archivos no reconocido)	
2.133	Capacidad para aplicar políticas granulares basadas en la actividad del usuario de la aplicación en la nube (en línea en tiempo real): carga de archivos, archivo adjunto, descarga de archivos	
2.134	La solución debe poder aplicar políticas de DLP por aplicaciones en la nube	
2.135	La solución debe tener la capacidad de crear políticas DLP basadas en diferentes predicados, como la ubicación, la funcionalidad de las aplicaciones en la nube, la inscripción de dispositivos (administrados o no administrados),	
2.136	La solución debe tener la capacidad de aplicar políticas basadas en el puntaje de impacto comercial que consiste en una regla de detección básica con un puntaje numérico, y estos puntajes se dividen en cuatro niveles diferentes: Crítico, Alto, Medio, Bajo.	

2.137	La solución debe admitir aplicaciones en la nube personalizadas en línea (HTTPS) sin necesidad de abrir una solicitud de función, y también debe admitir la protección DLP para carga/descarga	
2.138	Capacidad para admitir cualquier aplicación en la nube en línea (HTTPS) sin necesidad de abrir una solicitud de función con el oferente, y también debe admitir la protección DLP para carga/descarga	
2.139	La solución debe tener diferentes tipos de modos de implementación: API, integración de SSO a través de SAML 2.0 o instalación de agente	
2.140	La solución debe tener soporte para agregar proxy inverso al realizar la integración de SSO a través de SAML 2.0	
2.141	Capacidad para admitir la protección sin agente al acceder desde dispositivos no administrados	
2.142	La solución debe proporcionar análisis de comportamiento de riesgo del usuario en función de las actividades de los usuarios de aplicaciones en la nube	
2.143	Capacidad para admitir reglas de detección de anomalías para aplicaciones en la nube: fuerza bruta, apropiación de cuentas, información privilegiada malintencionada y comprometida y actividad sospechosa por parte de un usuario privilegiado.	
No.	**CAPACIDAD DATO EN REPOSO**	**CUMPLE/ NO CUMPLE**
2.144	La solución debe admitir el escaneo de datos en reposo para Exchange, Outlook PST, bases de datos, Sharepoint y sistemas de archivos	
2.145	La solución debe ser compatible con SMB, NFS y CIFS para recursos compartidos de archivos basados en Windows y no basados en Windows	
2.146	La solución debe ser compatible con los métodos de escaneo TCP o ICMP al buscar recursos compartidos de red	
2.147	Las tareas de descubrimiento de datos deben tener una opción de programación por: una vez, diaria, semanal o continuamente	
2.148	La tarea de descubrimiento de datos debe admitir la inclusión y exclusión por tipo de archivo, carpetas, edad o tamaño	
2.149	La tarea de descubrimiento de datos debe admitir opciones de escaneo diferencial y completo	
2.150	El descubrimiento de datos debe tener una opción para preservar el tiempo de acceso original	
2.151	El descubrimiento de datos debe admitir la asignación de ancho de banda para el escaneo del proceso de descubrimiento	
2.152	El descubrimiento de datos debe ser compatible con las capacidades de reconocimiento óptico de caracteres (OCR)	
No.	**CAPACIDAD DE GESTIÓN DE INCIDENTES**	**CUMPLE/ NO CUMPLE**
2.153	La solución debe proporcionar la capacidad de escalar los incidentes críticos a los administradores o propietarios de datos	
2.154	La solución debe proporcionar seguridad y controles de acceso en torno al caso/incidente (usuario y grupo)	

2.155	La solución debe asignar incidentes/casos a usuarios de diferentes Unidades de Negocio	
2.156	La solución debe permitir la definición y el establecimiento de flujos de trabajo específicos (es decir, agregar los tres tipos de eventos a los casos), asigna casos a usuarios/propietarios individuales, permite que los usuarios agreguen notas, etc.	
2.157	La solución debe respaldar el monitoreo y la gestión de los aspectos críticos y las fases de cada incidente/caso y las fases de cada incidente/caso hasta su resolución, involucrando a los administradores autorizados especificados y a los usuarios con roles específicos según se requiera durante todo el proceso.	
2.158	La solución debe proporcionar la capacidad de mostrar solo ciertos incidentes de un departamento en particular al punto focal asignado de ese departamento	
2.159	La solución debe proporcionar la capacidad de liberar automáticamente un correo electrónico en cuarentena, con la aprobación del administrador de publicación sin ninguna intervención manual dentro de la consola DLP.	
2.160	La solución debe admitir secuencias de comandos de remediación para los planes de acción de DLP (por ejemplo, cuando un archivo infringe las políticas de DLP, las soluciones dejan un archivo de desecho con una notificación)	
No.	**CAPACIDAD DE INFORMES, ALERTAS Y ANALISIS FORENSE**	**CUMPLE/ NO CUMPLE**
2.161	La solución debe permitir la investigación de incidentes relacionados con datos en reposo, datos en uso y datos en movimiento desde una consola de administración centralizada.	
2.162	La solución debe proporcionar resúmenes y agrupaciones de informes personalizados a través de diferentes variables y atributos.	
2.163	La solución debe admitir la exportación de informes de incidentes a través de una hoja de cálculo, XML, PDF o HTML.	
2.164	La solución debe tener informes predefinidos para ayudar en las investigaciones.	
2.165	La solución debe admitir la capacidad de guardar informes personalizados y filtros de incidentes.	
2.166	La solución debe admitir la capacidad de establecer permisos de informes por departamentos.	
2.167	La solución debe usar análisis de datos avanzados para proporcionar a su equipo de operaciones de seguridad un informe clasificado por pila sobre los principales riesgos de seguridad de datos dentro de su organización.	
2.168	La solución debería poder generar informes programados	
2.169	La solución debe proporcionar informes de incidentes flexibles (diarios, semanales, mensuales, trimestrales, etc.)	
2.170	La solución debería poder informar el número de alertas generadas por destino	
2.171	La solución debería permitir a los usuarios crear mensajes de alerta personalizables para administradores, usuarios y gerentes de usuarios.	
2.172	La solución debe proporcionar un catálogo de informes completo que proporcione un "desglose" para facilitar la investigación de los incidentes de mayor riesgo	
2.173	La solución debe ser capaz de proporcionar datos forenses dentro del mismo registro de incidentes.	

2.174	La solución debe priorizar instantáneamente los casos de niveles de riesgo alto a bajo con umbrales de puntaje de riesgo personalizables entregados en una pila de informes de clasificación de riesgo de incidentes	
2.175	La solución debe capturar datos de eventos con metadatos apropiados (fecha/hora, usuario, protocolo)	
2.176	La solución debe admitir un protocolo de cadena de custodia	
2.177	La solución debe conservar los registros al menos durante un año; si no es posible, la solución debe admitir el archivo de incidentes	
2.178	La solución debe tener la capacidad de cambiar la gravedad (Alta, Media, Baja) y el estado (Nuevo, En proceso, Cerrado, Falso positivo, Escalado)	
3. MÓDULO ETIQUETADO Y CLASIFICACIÓN DE INFORMACIÓN		
No.	**CAPACIDAD DE ETIQUETADO Y CLASIFICACIÓN**	**CUMPLE/ NO CUMPLE**
3.1	La solución debe tener la posibilidad de seleccionar la clasificación con un solo botón	
3.2	La solución debe tener la posibilidad de seleccionar la clasificación de una lista desplegable	
3.3	La solución debe tener la posibilidad de elegir más de un valor de clasificación (selecciones múltiples)	
3.4	La solución debe tener la posibilidad de aplicar varias etiquetas con un solo clic	
3.5	Los niveles del selector de clasificación se pueden anidar en el menú de la cinta	
3.6	Se puede pedir a los usuarios que clasifiquen mediante un cuadro de diálogo emergente	
3.7	Etiquetado asistido que guía al usuario a través de opciones de clasificación para garantizar selecciones válidas	
3.8	Opciones de clasificación etiquetadas dinámicamente para esquemas avanzados (como ITAR, CUI)	
No.	**GUIA DEL USUARIO**	**CUMPLE/ NO CUMPLE**
3.9	Los usuarios pueden crear y nombrar sus propias selecciones de clasificación 'favoritas'	
3.10	La solución debe tener la Posibilidad de tener una clasificación predeterminada o una clasificación sugerida	
3.11	Capacidad para que los usuarios establezcan su propia clasificación predeterminada o sugerida	
3.12	Interfaz de clasificación disponible en la barra de cinta de las aplicaciones de correo electrónico, Office y CAD	
3.14	Los usuarios pueden recibir información sobre herramientas que explicarán lo que significa cada opción de clasificación	
3.15	Botón de ayuda para vincular directamente a su política de clasificación	
3.16	Se le solicita al usuario que clasifique al guardar, imprimir o enviar un correo electrónico	
3.17	Los mensajes de diálogo de clasificación pueden ser compatibles con los idiomas locales.	
3.18	Se puede advertir a los usuarios o evitar que rebajen la clasificación	
3.19	La impresión se puede controlar en función de la clasificación y el contexto	
3.20	El usuario puede aplicar la clasificación masiva en varios archivos seleccionados en las vistas del explorador de archivos de Windows	

No.	CAPACIDAD DE APLICACIÓN MARCAS DE CLASIFICACIÓN DE ARCHIVOS	CUMPLE/ NO CUMPLE
3.21	Aplicar una marca al encabezado de un archivo	
3.22	Aplicar una marca al pie de página de un archivo	
3.23	Aplicar una marca de agua a un archivo	
3.24	Aplicar una marca de imagen a un archivo	
3.25	Aplicar una marca de cuadro de texto a un archivo	
3.26	Aplicar una marca de código de campo a un archivo	
3.27	Aplicar metadatos persistentes a un archivo	
3.28	Clasificar archivos que no admiten metadatos, por ejemplo, archivos TXT y CSV	
3.29	Las marcas visibles se pueden personalizar para que no afecten a las plantillas, el contenido existente, la estructura o la marca.	
3.30	Evita que el usuario guarde o imprima sin clasificar	
3.31	Evitar que el usuario envíe un correo electrónico sin clasificar	
3.32	Detenga la difusión accidental de correos electrónicos a los usuarios sin un nivel de autorización adecuado	
3.33	Sugiera u ordene una clasificación predeterminada basada en la posición de la empresa, el departamento, la ubicación y el contenido del archivo.	
3.34	Ordenar la clasificación de un archivo creado externamente cuando se abre, comparte o imprime	
3.35	Detectar archivos anidados en un archivo o el cuerpo de un correo electrónico	
3.36	Detectar contenido en archivos y sugerir u ordenar la clasificación	
3.37	Detecte contenido en archivos anidados y sugiera u ordene la clasificación	
No.	**CAPACIDAD INTEGRACIÓN DE CLASIFICACIÓN CON CORREO ELECTRÓNICO**	**CUMPLE/ NO CUMPLE**
3.38	La clasificación se puede aplicar en MS Outlook	
3.39	La clasificación se puede aplicar a la última versión de IBM Notes	
3.40	Cuando se clasifica un correo electrónico, los destinatarios y el autor se verifican automáticamente al enviarlos para garantizar que sean apropiados, por ejemplo, para evitar que un correo electrónico marcado como 'interno' vaya a un dominio externo.	
3.41	La clasificación se aplica automáticamente en función de atributos como si se incluyen todos los destinatarios de correo electrónico internos o una cierta cantidad de destinatarios.	
3.42	El nivel de clasificación de un correo electrónico se actualiza automáticamente para coincidir con el nivel de cualquier archivo adjunto (o coincidir con el nivel más alto de clasificación si hay más de un archivo adjunto)	
3.43	Los archivos adjuntos se pueden verificar para asegurarse de que estén clasificados y que la clasificación no haya vencido	
3.44	Todos los destinatarios se pueden verificar individualmente con atributos como los de Active Directory	
3.45	La clasificación puede verificar cuántos destinatarios hay en el correo electrónico	
3.46	La clasificación de un correo electrónico se puede conservar en la respuesta de un destinatario externo	
3.47	Aplicar marcas en la primera línea de texto	

3.48	Aplicar marcas en la última línea de texto	
3.50	Aplicar marcas en el asunto de un correo electrónico como prefijo o adjunto	
3.51	Aplicar marcas en el encabezado x de un correo electrónico	
3.52	Aplicar cifrado S/MIME	
3.53	Agrega detalles de los archivos adjuntos (incluida su clasificación) al final de un correo electrónico, proporcionando un historial de archivos adjuntos	
3.54	Los 'recibos de lectura' pueden ser controlados por clasificación	
3.55	La clasificación puede cambiar la importancia o la confidencialidad de un correo electrónico	
3.56	Añadir una fecha de caducidad a un correo electrónico	
3.57	Agregar una dirección de correo electrónico según la clasificación	
3.58	Agregar una categoría de Outlook a un correo electrónico	
3.59	Aplicar la gestión de derechos (por ejemplo, Azure RMS, Seclore, Sealpath)	
3.60	La clasificación puede controlar la longitud del asunto del correo electrónico	
3.61	La clasificación puede controlar el tamaño de un mensaje.	
3.62	La clasificación puede controlar 'responder a todos'	
No.	**CAPACIDAD DE REGISTRO DE LOGS**	**CUMPLE/ NO CUMPLE**
3.63	Los metadatos son persistentes: los metadatos eliminados se vuelven a aplicar cuando el archivo se guarda, se imprime o se envía por correo electrónico.	
3.64	Se puede evitar que los usuarios cambien la clasificación	
3.65	Se registran los datos del usuario que clasificó el archivo	
3.66	Si un usuario puede cambiar la clasificación, este cambio se registrará	
3.67	Todas las acciones de clasificación se registran	
3.68	Se puede acceder al registro de eventos registrados con fines de investigación o auditoría	
3.69	Los eventos se pueden reenviar a la base de datos de informes del clasificador o a cualquier solución de informes y análisis de terceros.	
3.70	Una solución de informes dedicada está disponible	
3.71	Los informes se pueden personalizar	
3.72	Los tableros se pueden configurar para reflejar información importante del registro de eventos	
No.	**CAPACIDAD GESTIÓN DE POLÍTICAS**	**CUMPLE/ NO CUMPLE**
3.73	La solución posea una sencilla herramienta de gestión donde se pueden crear y modificar políticas	
3.74	Las reglas de política se pueden crear y editar con un asistente simple	
3.75	Las políticas se pueden personalizar con una amplia gama de atributos, por ejemplo, atributos de Active Directory.	
3.76	Sin límite en el número de políticas que se pueden crear	
3.77	Niveles de clasificación ilimitados para permitir que una póliza evolucione	
3.78	La clasificación se puede modificar con el tiempo, a medida que se desarrollen las necesidades comerciales.	
3.79	Las políticas pueden alinearse con las políticas internas de marcado y aplicación de una empresa	

3.80	Se puede aplicar una variedad de elementos de clasificación, por ejemplo, selectores únicos, selectores múltiples, selectores de fecha, desplazamiento de fecha o texto libre.	
3.81	Las políticas se pueden probar fácilmente (modo de prueba) antes de la implementación	
3.82	La clasificación puede ser obligatoria	
3.83	Las políticas se pueden adaptar para diferentes departamentos o jerarquías; por ejemplo, solo los gerentes pueden degradar una clasificación.	
3.84	Las reglas se pueden adaptar para diferentes departamentos o jerarquías; por ejemplo, las marcas visibles no aparecen en un archivo cuando se imprime si el usuario está en Marketing.	
3.85	Los menús de clasificación se pueden adaptar para diferentes departamentos o jerarquías	
3.86	Los botones de clasificación se pueden envolver (apilar) en columnas de 3 (para que no ocupen demasiado espacio en la cinta)	
3.87	Se admite la localización del idioma.	
3.88	El soporte de idiomas está automatizado en función de la ubicación del usuario.	
No.	**INFRAESTRUCTURA Y CAPACIDAD**	**CUMPLE/ NO CUMPLE**
3.89	La clasificación no "hincha" un archivo clasificado, haciéndolo sustancialmente más grande	
3.90	Las políticas no requieren grandes archivos de configuración	
3.91	Tiene una demanda de infraestructura mínima, por ejemplo, no requiere tecnología de base de datos y las políticas se pueden distribuir por archivo	
3.92	Se admiten implementaciones en varios sitios	
3.93	Funciona sin conexión, por lo que no impedirá que los empleados puedan trabajar	
3.94	Si está fuera de línea por algún motivo, aún registrará las acciones del usuario para una revisión posterior	
3.95	Los metadatos del clasificador pueden ser detectados por procesos de descubrimiento para ayudar a localizar archivos o sensibilidad particular	
3.96	Las plantillas, las marcas preexistentes y la ubicación del archivo se pueden usar como condiciones para la clasificación automática	
3.97	Las herramientas de descubrimiento pueden leer fácilmente la clasificación para garantizar que el archivo se almacene en una ubicación adecuada	
3.98	Soporte para Windows Vista o posterior	
3.99	Compatibilidad con Microsoft Office 2007 SP3 o posterior	
3.100	Compatibilidad con SharePoint 2010 o posterior	
3.101	Soporte para OWA 2010 o posterior	
3.102	Compatibilidad con Exchange 2010 o posterior	
3.103	Aplique marcas visuales y metadatos a MS Outlook	
3.104	Aplique marcas visuales y metadatos a MS Office (Word, Excel, PowerPoint)	
3.105	Aplicar marcas visuales y metadatos a MS Project	
3.106	Aplicar marcas visuales y metadatos a MS Visio	
3.107	Aplicar metadatos persistentes a un archivo de Open Office (SO Windows)	
3.108	Aplicar metadatos persistentes a un PDF (SO Windows)	

3.109	Aplicar metadatos persistentes a JPEG, PNG, TIFF y otros archivos de imagen (SO Windows)	
3.110	Aplicar metadatos persistentes a archivos de correo electrónico MSG y EML (SO Windows)	
3.111	Aplicar metadatos persistentes a un archivo ZIP (SO Windows)	
3.112	Aplique metadatos persistentes a archivos CAD DWG y DXF (SO Windows)	
3.113	Aplicar metadatos persistentes a un archivo HTML (SO Windows)	
3.114	Puede clasificar archivos que no admiten metadatos	
3.115	Aplicar clasificación para SharePoint	
3.116	Ver clasificación de archivos para SharePoint	
3.117	Cambiar clasificación para SharePoint	
3.118	Realizar clasificación por lotes para SharePoint	
3.119	Realice una clasificación masiva basada en un proceso por lotes o una secuencia de comandos de corrección para SharePoint	
3.120	Ponga en cuarentena los archivos "confidenciales" si se cargan en una biblioteca pública para ocultarlos de la vista de SharePoint	
3.121	Compatible con OSX para Mac	
3.122	Clasificar en versiones Mac de MS Office (Word, PowerPoint, Excel)	
3.123	Clasificar en versiones Mac de MS Outlook	
3.124	Los archivos conservan la clasificación si se abren en una versión basada en navegador de una aplicación	
3.125	Los correos electrónicos se pueden clasificar en la aplicación web de Outlook (OWA), utilizando Exchange local o Exchange Online (Office 365)	
3.126	La solución OWA puede aplicar marcas visuales a un correo electrónico	
3.127	La solución OWA puede aplicar metadatos a un correo electrónico	
3.128	La solución OWA puede verificar los destinatarios de los mensajes de correo electrónico	
3.129	La solución OWA puede verificar la clasificación de los archivos adjuntos de correo electrónico	
3.130	Interoperabilidad con proveedores de CASB que permite el control basado en metadatos de clasificación	
3.131	Integración con soluciones de almacenamiento en la nube (por ejemplo, Box)	
3.132	Los archivos conservan la clasificación si se abren en un móvil	
3.133	Funcionalidad para clasificar correos electrónicos en un dispositivo Windows Phone	
3.134	Funcionalidad para clasificar correos electrónicos en un dispositivo iOS	
3.135	Funcionalidad para clasificar correos electrónicos en un dispositivo Android	
3.136	Interoperabilidad con proveedores de mensajería móvil (p. ej., Blackberry, Citrix ZenMobile, MobileIron, VMware AirWatch)	
3.137	Compatibilidad con el almacenamiento de archivos de Windows	
3.138	Soporte para almacenamiento Samba (Linux)	
3.139	Interoperabilidad con soluciones de prevención de pérdida de datos	
3.140	Interoperabilidad con Data Discovery (Gobernanza)	
3.141	Interoperabilidad con soluciones de monitoreo, informes y análisis	
3.142	Interoperabilidad con soluciones de administración de derechos	

3.143	Interoperabilidad con soluciones de control de acceso	
3.144	Interoperabilidad con soluciones de filtrado de correo electrónico	
3.145	Interoperabilidad con soluciones de correo electrónico seguro	

4. COMPATIBILIDAD, SOPORTE, MANTENIMIENTO Y LICENCIAMIENTO GENERAL		
No.	**COMPATIBILIDAD DE LOS MÓDULOS**	**CUMPLE/ NO CUMPLE**
4.1	El cliente para la instalación en estaciones de trabajo debe ser compatible con los siguientes sistemas operativos: - Apple MacOS 10.15.x. - Apple MacOS 11.1 a 11.5. - Citrix XenDesktop. - Windows 10 (incluyendo 21H1). - Windows 8.1. - Windows Server 2012 R2. - Windows Server 2016. - Windows Server 2019.	
4.2	Debe permitir la distribución del agente a través de herramientas de terceros, tales como: - GPO. - IBM Tivoli. - Microsoft System Center. - Manage Engine - Symantec Client Management Suite	
4.3	Debe tener mecanismos para evitar que el usuario detenga los servicios del agente.	
4.4	Debe brindar al menos un mecanismo de protección para evitar que el usuario final desinstale el cliente.	
No.	**SOPORTE, MANTENIMIENTO Y LICENCIAMIENTO GENERAL**	**CUMPLE/ NO CUMPLE**
4.5	El nivel de servicios (SLA) de mantenimiento y soporte para la solución con ambos módulos, deberá ser de 24*7*365	
4.6	El alcance de licenciamiento es: - Un Total de 1,150 usuarios (agentes o conectores DLP) - De ese total, solo 750 usuarios tendrán capacidad de clasificar información. -Dos (2) años de licenciamiento o suscripción de la solución DLP y clasificación de la información.	

5. CAPACITACIONES Y ENTRENAMIENTOS		
No.	**CAPACITACIONES**	**CUMPLE/ NO CUMPLE**

5.1	**CAPACITACIÓN ADMINISTRACIÓN PLATAFORMA:** El oferente a través del fabricante de la marca de la solución con sus módulos, debe capacitar al siguiente personal técnico: - Tres (3) Usuarios Sección Seguridad de Información - Dos (2) Usuarios Dirección Operaciones	
5.2	**CAPACITACIÓN PARA USUARIOS CLASIFICADORES INFORMACIÓN:** El oferente a través del fabricante de la marca de la solución con sus módulos debe capacitar al siguiente personal que va a clasificar las informaciones con la solución: - Veinticinco (25) Usuarios Finales de las Direcciones con informaciones más críticas. - Crear manual de enseñanza de clasificación de la información.	

CONDICIONES TECNICAS ESPECIALES DEL OFERENTE		
No.	**A) COMPETENCIAS DE LA EMPRESA OFERENTE *(REQUERIDO)***	**CUMPLE / NO CUMPLE**
1	El oferente de la solución con sus módulos debe presentar certificación de la solución, indicando que el mismo, está autorizado a ser representante directo de la marca ofertada en República Dominicana. (Se validará directamente con el fabricante).	
2	El oferente de solución con sus módulos debe presentar una certificación por parte del fabricante indicando que está certificado para vender e instalar los componentes propuestos a el Banco Agrícola. (Se validará directamente con el fabricante).	
No.	**COMPETENCIAS DE LA EMPRESA OFERENTE *(PUNTUACION)***	**PUNTUACIÓN**
3	El oferente debe poseer años de experiencia demostrada ofreciendo consultoría e implementando este tipo de proyectos. El puntaje se determina de la siguiente manera, presentando carta o certificaciones que abalen sus años de experiencia en consultoría e implementando proyectos de solución DLP o proyectos de soluciones de ciberseguridad: - **6 años o más** de experiencia. **Valor 20 Puntos.** - **Entre 4 a 5 años** de experiencia. **Valor 14 Puntos**. - **Entre 2 a 3 años** de experiencia. **Valor 10 Puntos.** **NOTA: Las cartas o certificaciones, deben poseer los siguientes datos:** - Nombre de la empresa donde se implementó la solución de ciberseguridad. - Nombre y contacto teléfono y Email del líder técnico del proyecto en la empresa. - Sello y firma de la empresa.	**20**

4	El oferente debe incluir evidencia de proyectos en los cuales haya implementado solución DLP, de manera local o internacional. El puntaje se determina de la siguiente manera: - **3 o más cartas** de clientes donde hayan implementado solución DLP. **Valor 25 Puntos.** - **2 cartas** de clientes donde hayan implementado solución DLP. **Valor 15 Puntos.** - **Mínimo requerido de 1 carta** de cliente donde haya implementado solución DLP. **Valor 10 Puntos.** **NOTA: Las cartas, deben poseer los siguientes datos:** - Nombre de la empresa donde se implementó la solución DLP. - Nombre y contacto teléfono y Email del líder técnico del proyecto en la empresa. - Sello y firma de la empresa.	**25**
No.	**COMPETENCIAS PROFESIONALES DEL PERSONAL**	**PUNTUACIÓN**
5	**ROL: GERENTE DE PROYECTO (PROJECT MANAGER).** Se requiere asignar un gerente de proyecto, el cual se encargue de llevar la gestión del proyecto de acuerdo con una metodología de manejo de proyectos avalada por el Project Management Institute. - Titulo de Lic. o Ingeniero de Adm. Empresas, Sistemas, Industrial o afines. - Mínimo 3 años de experiencia gestionado proyectos. - Debe contar con la **Certificación PMP vigente o equivalente de Project Management,** para el manejo del proyecto. - Cartas de experiencia de al menos 3 proyectos sobre soluciones DLP, soluciones de ciberseguridad o tecnológicos ejecutados. - Preparar y entregar informes diarios de seguimiento del proyecto. - Debe estar dedicado 100% onsite a este proyecto. **NOTA**: En caso de no presentar todos los requisitos establecidos, la puntación será cero (0).	**15**
6	**ROL: CONSULTOR SENIOR PROYECTO DLP** Se requiere un personal como consultor senior del proyecto DLP, el mismo, debe cumplir con el siguiente perfil de competencias: Esta persona se encargará de asesorar, orientar al personal técnico y ejecutivo, garantizando que los diferentes módulos de la solución, puedan operar como un único sistema integrado. - **Título de Ingeniero o Licenciado en Sistemas, Telemática o afines.** - **De 4 a 8 años mínimo de experiencia en el área de ciberseguridad o data privacy.** - **Certificación vigente técnica del producto o solución a implementarse** - **Certificación vigente de Data Privacy o Protección de Datos, ejemplos: GDPR, CDPSE, CDPP.** **NOTA**: En caso de no presentar todos los requisitos establecidos, la puntación será cero (0).	**20**

7	**Rol: Consultor Junior Proyecto DLP** Se requiere un personal como Consultor Junio del proyecto DLP, el mismo, debe cumplir con el siguiente perfil de competencias: Esta persona se encargará de apoyar en la orientación, implementación y capacitación al personal técnico que administraran la solución con sus módulos del DLP. **- Título de Ingeniero o Licenciado en Sistemas, Telemática o afines.** **- De 2 a 5 años mínimo de experiencia en el área de ciberseguridad o data privacy.** **- Certificación vigente técnica del producto o solución a implementarse** **- Certificación del área de ciberseguridad, ejemplos: CompTIA Security+, CSX ISACA Fundamental, otras afines.** **NOTA**: En caso de no presentar todos los requisitos establecidos, la puntación será cero (0).	**20**
	PUNTUACION TOTAL:	**100**

DIRECCIÓN DE CIBERSEGURIDAD Banco Agrícola

ENGEL RIVAS
DIRECTOR DE CIBERSEGURIDAD