ANEXO No. 1 ESPECIFICACIONES Y CONDICIONES TÉCNICAS

No.	Característica requerida	Descripción del requerimiento	Mínimo Requerido
1. ARQUITECTURA E INTEGRACIÓN			
1.1	**Integración nativa multi-plataforma**	La solución deberá integrarse nativamente con plataformas de correo electrónico en la nube, Microsoft 365, sin necesidad de redireccionamiento de registros MX.	**100%**
1.2	**Integración vía API con Microsoft 365**	La solución deberá soportar integración con Microsoft 365 a través de API como modalidad de conexión, permitiendo la configuración y el procesamiento del correo sin modificación de la ruta de entrega (registros MX). La INC se reserva la decisión sobre la modalidad de integración a implementar durante la ejecución del contrato, conforme a los requerimientos técnicos del entorno en producción.	**100%**
1.3	**Consola de administración centralizada en la nube**	La solución deberá ser administrada desde una consola centralizada en la nube que permita gestionar correo electrónico, endpoints, servidores, red y otros productos de seguridad desde un único panel.	**100%**
2. PROTECCIÓN CONTRA AMENAZAS Y MALWARE			
2.1	**Escaneo multicapa de malware, spam y ransomware**	La solución deberá contar con escaneo multicapa de malware, spam y ransomware en correos electrónicos entrantes, salientes y archivos adjuntos.	**100%**
2.2	**Sandbox en la nube para análisis dinámico**	Deberá incluir un espacio seguro en la nube (sandbox) para el análisis dinámico de archivos sospechosos, evaluando procesos, actividad de archivos, registros del sistema y conexiones de red.	**100%**
2.3	**Detección de amenazas Zero-Day con IA / Deep Learning**	La solución deberá soportar inteligencia artificial (Deep Learning / Machine Learning) para la detección de amenazas de día cero sin necesidad de firmas previas.	**100%**
2.4	**Bloqueo de URLs maliciosas en tiempo real**	Deberá detectar y bloquear URLs maliciosas en tiempo real antes de que el correo sea entregado al destinatario.	**100%**
2.5	**Reescritura de URLs — protección Time-of-Click**	La solución deberá reescribir las URLs al momento del clic (Time-of-Click) para evaluar el destino en el instante en que el usuario hace clic, bloqueando el acceso si la URL ha cambiado a estado malicioso.	**100%**
2.6	**Protección posentrega — eliminación automática de correos maliciosos**	Deberá ofrecer protección posentrega: capacidad de eliminar automáticamente correos maliciosos de la bandeja del usuario cuando el estado de amenaza de una URL cambia tras la entrega.	**100%**
2.7	**Trazabilidad y reportes de acciones posentrega**	La solución deberá generar reportes y trazabilidad de las acciones automáticas de protección posentrega, accesibles desde la consola de administración.	**100%**
2.8	**Inteligencia de amenazas acumulada (30+ años)**	La solución podrá estar respaldada por una plataforma de inteligencia de amenazas con amplia trayectoria en el sector de ciberseguridad, que incluya capacidades de análisis de reputación y comportamiento basadas en datos históricos acumulados.	**100%**
3. PROTECCIÓN CONTRA PHISHING Y SUPLANTACIÓN DE IDENTIDAD			
3.1	**Bloqueo de phishing sin malware y ataques BEC**	La solución deberá bloquear ataques de phishing sin malware (malware-free phishing) y estafas por correo electrónico corporativo comprometido (BEC — Business Email Compromise).	**100%**
3.2	**Protección reforzada para usuarios VIP**	Deberá identificar automáticamente los objetivos de alto perfil (usuarios VIP) de la organización para aplicar protecciones adicionales contra suplantación de identidad.	**100%**
3.3	**Análisis del nombre mostrado (Display Name) del remitente**	La solución deberá analizar el nombre mostrado (Display Name) del remitente para detectar impostores que se hagan pasar por ejecutivos, proveedores o entidades confiables.	**100%**
3.4	**Detección de dominios de imitación (look-a-like domains)**	Deberá incluir detección de dominios de imitación (look-a-like domains) que intentan suplantar el dominio legítimo de la organización o de terceros de confianza.	**100%**
3.5	**Análisis de contenido con NLP para detección de suplantación**	La solución deberá emplear análisis de contenido de mensajes mediante Procesamiento de Lenguaje Natural (NLP) para identificar patrones de suplantación y manipulación.	**100%**
4. AUTENTICACIÓN DE REMITENTES Y CUMPLIMIENTO DMARC			
4.1	**Validación SPF, DKIM y DMARC**	La solución deberá validar la autenticación de remitentes mediante los protocolos estándar SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting and Conformance).	**100%**
4.2	**Gestión de cumplimiento DMARC del dominio propio**	Deberá ofrecer herramientas para la gestión del cumplimiento DMARC del dominio propio de la organización, incluyendo generación de informes, gestión de registros DNS y automatización del proceso de implementación.	**100%**
4.3	**Compatibilidad con DANE y ARC**	La solución deberá ser compatible con los protocolos DANE (DNS-based Authentication of Named Entities) y ARC (Authenticated Received Chain) para garantizar el transporte seguro y la cadena de autenticación.	**100%**
4.4	**Verificación de identidad de remitentes autorizados**	Deberá permitir la verificación de identidad de remitentes autorizados, evitando que actores maliciosos suplanten dominios legítimos de la organización o de sus proveedores.	**100%**

5. PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) Y CIFRADO			
5.1	**DLP con políticas multi-regla por grupos y usuarios**	La solución deberá contar con capacidades de Prevención de Pérdida de Datos (DLP) con políticas de múltiples reglas configurables por grupos de usuarios y usuarios individuales.	**100%**
5.2	**Detección automática de información sensible (PII, financiera, médica)**	Deberá detectar automáticamente información sensible en cuerpos de mensajes y archivos adjuntos, incluyendo datos financieros, información médica y datos personales (PII).	**100%**
5.3	**Listas de control de contenido personalizables**	Deberá incluir listas de control de contenido personalizables para definir términos, patrones o tipos de datos cuya transmisión debe ser controlada o bloqueada.	**100%**
5.4	**Cifrado en tránsito con TLS forzado**	La solución deberá soportar cifrado de correos electrónicos con TLS forzado (Enforced TLS) para garantizar el transporte seguro de mensajes entre servidores.	**100%**
5.5	**Cifrado y firma digital S/MIME**	Deberá soportar cifrado y firma digital de mensajes mediante S/MIME para verificar la identidad del remitente y garantizar la integridad del mensaje.	**100%**
5.6	**Cifrado basado en imposición (push-based encryption)**	La solución deberá ofrecer cifrado basado en imposición (push-based encryption), donde el remitente envía el mensaje cifrado y el destinatario accede a través de un portal seguro.	**100%**
5.7	**Cifrado de adjuntos en formatos PDF y Office**	Deberá soportar cifrado de archivos adjuntos en formatos PDF y Microsoft Office como mecanismo adicional de protección de documentos sensibles.	**100%**
6. VISIBILIDAD, REPORTES Y GESTIÓN CENTRALIZADA			
6.1	**Paneles de control en tiempo real**	La solución deberá incluir paneles de control en tiempo real con información sobre el estado del correo electrónico, amenazas detectadas y actividad de usuarios.	**100%**
6.2	**Historial completo de mensajes con búsqueda avanzada**	Deberá ofrecer historial completo de mensajes procesados, con capacidad de búsqueda y filtrado por remitente, destinatario, fecha, estado y tipo de amenaza.	**100%**
6.3	**Informes de URLs bloqueadas, con advertencia y permitidas**	La solución deberá generar informes de URLs bloqueadas, URLs con advertencia y URLs permitidas en el momento del clic, con estadísticas de volumen.	**100%**
6.4	**Informes de infracciones de políticas DLP**	Deberá incluir informes de infracciones de políticas DLP, con detalle de mensajes registrados y tipo de dato sensible detectado.	**100%**
6.5	**Reportes de sandbox con MITRE ATT&CK**	La solución deberá generar informes de amenazas avanzadas detectadas en el sandbox, incluyendo resultados de análisis externo de reputación y tácticas de la matriz MITRE ATT&CK.	**100%**
6.6	**Resumen de actividad posentrega**	Deberá incluir resumen de actividad posentrega, mostrando los mensajes eliminados automáticamente por cambio en el estado de amenaza de URLs ya entregadas.	**100%**
6.7	**Gestión del ciclo de vida de licencias y reportes de uso**	La consola de administración deberá permitir gestionar el ciclo de vida de licencias e incluir reportes de uso.	**100%**
7. INTEGRACIÓN CON PLATAFORMAS XDR Y MDR			
7.1	**Integración con plataforma XDR para correlación de eventos**	La solución deberá soportar la integrarción con una plataforma de Detección y Respuesta Extendida (XDR) para correlacionar eventos de seguridad del correo electrónico con eventos de endpoints, servidores y red.	**100%**
7.2	**Ingesta de eventos de correo en Data Lake XDR**	Los eventos de seguridad del correo (intentos de compromiso de cuentas, DLP, protección posentrega) deberán soportar la ingesta en el Data Lake de la plataforma XDR para análisis por analistas de seguridad.	**100%**
7.3	**Compatibilidad con servicio MDR gestionado**	La solución podrá soportar compatibilidad con un servicio de Detección y Respuesta Administrada (MDR) que permita el analisis de eventos críticos de correo, incluyendo la recuperación de mensajes maliciosos y el bloqueo de remitentes, dominios o IPs maliciosas.	**100%**
7.4	**Visibilidad extendida a M365, servidores, móviles y red**	La integración XDR podrá soportar la extensión de la visibilidad a cargas de trabajo de Microsoft 365, servidores, dispositivos móviles y red, desde un único Data Lake centralizado.	**100%**
8. CRITERIOS DE EXPERIENCIA, SOPORTE Y RECONOCIMIENTO			
8.1	**Evaluaciones independientes de laboratorio vigentes**	El fabricante de la solución deberá contar con evaluaciones independientes de detección de amenazas por laboratorios especializados (p. ej. VBSpam, SE Labs u otros equivalentes), con resultados publicados en los últimos 12 meses.	**100%**
8.2	**Reconocimiento por analistas de la industria (Gartner / Forrester / KuppingerCole)**	La solución deberá haber sido reconocida por al menos un analista de la industria de ciberseguridad (Gartner, KuppingerCole, Forrester u otros equivalentes) en informes publicados en los últimos 24 meses.	**100%**
8.3	**Experiencia demostrable en organizaciones con más de 200 usuarios**	El oferente deberá demostrar experiencia en implementación de soluciones de seguridad de correo electrónico en organizaciones del sector público o privado con más de 200 usuarios.	**100%**
8.4	**Soporte técnico en español para América Latina con SLA definidos**	La solución propuesta deberá contar con soporte técnico en español disponible para América Latina, con tiempos de respuesta definidos por nivel de severidad.	**100%**
Total de requisitos: 42			