ANEXO 2 - REQUISITOS SOFTWARE

Nombre contacto:	0
Correo electrónico contacto:	0
Cargo:	0
Teléfono contacto:	0
Fecha:	

CRITERIO	CÓDIGO	REQUERIMIENTO	CUMPLE	OBSERVACIONES DEL PROVEEDOR	EVIDENCIAS DEL PROVEEDOR	OBSERVACIONES ORGANIZACIÓN CONTRATANTE
SEGURIDAD EN EL DESARROLLO	RS-SD-01	¿Se ha a llevar a cabo desarrollo de software como parte de las actividades objeto del contrato?				
	RS-SD-02	En caso afirmativo a la pregunta "RS-SD-01", ¿dispone el proveedor de una metodología y practica de desarrollo seguro? En caso de realizar tareas de mantenimiento, el proveedor disponer igualmente de una metodología de desarrollo seguro.				
	RS-SD-03	¿El proveedor dispone de una separación entre los entornos de producción y los de desarrollo o integración?				
	RS-SD-04	¿El proveedor revisa, al menos anualmente, los privilegios de los desarrolladores de sistemas?				
	RS-SD-05	¿El proveedor dispone de un SBOM (Software bill of materials)? En caso afirmativo, debe proporcionar este registro formal y estructurado de la composición del software.				
	RS-SD-06	¿El proveedor emplea mecanismos para anonimizar/enmascarar datos reales con el objetivo de utilizarlos en entornos pre-productivos (desarrollo, pruebas, etc.)?				
CIBERDEFENSA	RS-CB-01	¿El proveedor va a proveer a la empresa de un software como objeto del contrato?				
	RS-CB-02	En caso afirmativo, ¿el proveedor ha realizado un escaneo de vulnerabilidades del mismo, y dispone de un proceso formal para la resolución de vulnerabilidades detectadas, de acuerdo a la criticidad de estas? El proveedor debe facilitar el resultado de este escaneo.				
	RS-CB-03	El proveedor debe hacerse cargo de la resolución de las vulnerabilidades que afecten a los sistemas de información del servicio que provean.				
	RS-CB-04	¿El proveedor ha habilitado los mecanismos de configuración, generación, almacenamiento, custodia y entrega de registros de trazabilidad de acceso y uso a los activos de información bajo su alcance?				
	RS-CB-05	Los logs se entregarán al SIEM de la empresa contratante, en las instalaciones de la empresa contratante o bien en su defecto, si la empresa lo autoriza, la entrega e integración sería sustituida por una API que el proveedor pondría a disposición de la empresa para la captura de los logs por parte del SIEM. Es responsabilidad del proveedor garantizar que la ingesta en el SIEM se realiza de forma correcta.				
	RS-CB-06	¿El proveedor ha dotado a la plataforma de protección frente ataques de denegación de servicio a nivel de red y de aplicación?				
	RS-CB-07	¿El proveedor garantiza que, los relojes de todos los sistemas de información asociado al servicio prestado, se sincronizarán con una fuente de tiempo exacta acordada previamente?				
SEGURIDAD DE LOS DATOS	RS-DA-01	¿El proveedor dispone de los oportunos mecanismos de cifrado de información en tránsito, en uso y almacenada?				
	RS-DA-02	¿De qué mecanismos criptográficos dispone el proveedor?				
	RS-DA-03	¿El proveedor dispone de una estrategia para la seguridad de las comunicaciones, incluyendo la segregación de redes por zonas de confianza, filtrado de tráfico de red y cifrado en los segmentos en que se requiera?				
	RS-DA-04	¿El proveedor dispone de segregación para los datos de las distintas empresas de forma que estén segregados de forma física para los diferentes clientes?				
GESTIÓN DE LA IDENTIDAD	RS-GI-01	¿El servicio permite que la autenticación se integre con los sistemas de autenticación de la empresa? Para ello, el proveedor garantizará que el servicio soporta mecanismos de federación de la identidad basado en buenas prácticas y estándares del mercado (SAML2, ADFS, etc.).				

	RS-GI-02	¿El proveedor garantiza que aplica el criterio de mínimo privilegio mediante la capacidad para dotar a los diferentes usuarios de permisos adecuados para realizar acciones previstas para sus correspondientes perfiles?				
SERVICIOS EN LA NUBE	**RS-SN-01**	¿El proveedor cuenta con los siguientes productos de seguridad para el software objeto del alcance del contrato?:				
		a.Defensa perimetral y perímetro virtual (FW, etc.).				
		b.Protección IDS e IPS.				
		c.Antimalware.				
		d.UEBA.				
		e.Solución de Seguridad de filtrado a nivel de aplicación.				
		f.Cuando la naturaleza de la solución incorpore servicios web, protección de aplicaciones (WAF).				
		g.En su caso, soluciones de protección CASB.				
		h.Cuando incorpore información sensible o confidencial, solución tipo DLP.				
		i.Cuando requiera navegación web, proxys de Navegación.				
		j.Cuando la naturaleza de la solución incorpore envío y recepción de correo electrónico, se requerirán medidas de protección de correo (antimalware, antispam, reputación…).				
		k.Cuando se trate de servicios expuestos a Internet, doble factor de autenticación. Indicar el producto con el cuenta para cubrir cada uno de estos apartados.				
	RS-SN-02	Antes de entrar en producción, y al menos una vez al año, ¿el proveedor de servicios en la nube proporciona una certificación exitosa de pruebas de penetración/actividad de hacking ético, por una entidad externa reconocida con el fin de garantizar que los controles de seguridad estén activos y sean efectivos en todo el perímetro del servicio ofrecido a la empresa contratante?				
	RS-SN-03	¿Los centros de datos/salas de servidores en su caso, donde se almacenan los datos están situados en países de la Unión Europea?				
	RS-SN-04	El proveedor, para todos los servicios en la nube objeto del contrato, debe indicar: a.**E**mpresa proveedora encargada de alojar el servicio en la nube. b.**D**ireccionamiento IP. c.**P**uertos requeridos para la provisión del servicio. d.**G**eolocalización de cada uno de los servicios prestados. e.**P**lataforma de protección de aplicaciones nativa en la nube de la que dispone.				
	RS-SN-05	El proveedor de servicios en la nube, ¿proporciona funciones al cliente que le permitan gestionar los activos de su propiedad?				
INTELIGENCIA ARTIFICIAL	**RS-IA-01**	¿La solución limita la funcionalidad y los permisos del complemento/herramientas del modelo de inteligencia Artificial?				
	RS-IA-02	¿La solución registra y monitorea la actividad de los complementos/herramientas del modelo de inteligencia artificial y los sistemas posteriores?				
	RS-IA-03	¿El proveedor supervisa la utilización de recursos de inteligencia artificial para identificar un posible ataque DoS?				
	RS-IA-04	¿El proveedor garantiza que el modelo de Inteligencia Artificial se verifica y firma digitalmente?				
	RS-IA-05	¿La solución proporciona una política de aplicación de parches para componentes obsoletos o vulnerables?				
	RS-IA-06	En caso de que el modelo de Inteligencia Artificial haya sido entrenado o ajustado con información confidencial, ¿se han empleado técnicas para abordar una posible divulgación de información confidencial?				
	RS-IA-07	¿La solución implementa filtrado de entrada, categorías de fuentes de datos y técnicas de saneamiento de datos para los datos que provienen de fuentes externas?				
	RS-IA-08	La solución deberá cumplir con todas las regulaciones y leyes. Se realizará una evaluación certificada en la etapa de desarrollo del modelo para garantizar que el modelo cumple con la regulación.				

	RS-IA-09	¿El proveedor dispone de alguna certificación relacionada con IA: ISO 42001:2023, Sistema de Gestión de Inteligencia Artificial? En caso afirmativo, se deben entregar a la empresa contratante las certificaciones o evaluaciones de cumplimiento para verificar que la solución cumple con las regulaciones aplicables.				