

FORMULARIO DE REQUISITOS DE SEGURIDAD Y CONTINUIDAD

FREMAP exige a sus proveedores la adopción de principios comunes alineados con su Política de Seguridad de la Información y su Política de Continuidad de Negocio, conforme a los estándares establecidos en las normas ISO 27001, ISO 22301 y el Esquema Nacional de Seguridad en su nivel ALTO.

El proveedor receptor de esta solicitud deberá responder conforme a la solución que va a implantar, aportando el mayor nivel de detalle posible de forma concisa, clara y coherente, de acuerdo al cumplimiento obligatorio de las medidas de seguridad y continuidad expresadas en los requisitos del pliego, en la Política de Seguridad de FREMAP y en la Política de Continuidad de FREMAP.

Las respuestas proporcionadas se considerarán un compromiso formal por parte del proveedor ante posibles reclamaciones legales derivadas de incidentes de seguridad que afecten directa o indirectamente a FREMAP. Así mismo, el proveedor estará obligado a comunicar formalmente cualquier cambio en su operación, servicio o infraestructura que pueda impactar en los servicios o en la información de FREMAP.

Adicionalmente, y en función del nivel de criticidad del proveedor, FREMAP podrá requerir información complementaria con el fin de evaluar su capacidad en materia de seguridad de la información, gestión del riesgo, operación del servicio y continuidad de negocio.

1. DIAGRAMA CONCEPTUAL DE LA SOLUCIÓN.

Se deberá adjuntar un dibujo/diagrama del sistema desde el puesto de trabajo hasta todos los componentes físicos/lógicos de la solución. Especificar qué tipos de sistema son hardware o sistemas cloud IAS o SAS.

Especificar un segundo diagrama con los esquemas de comunicación lógica entre los distintos componentes del sistema.

<INSERTAR DIAGRAMAS>

2. CARACTERÍSTICAS HARDWARE

Indicar si la solución propuesta requiere de equipamiento informático y sus características. También especificar si son servidores virtuales en cloud o servicio SAS en los campos más adecuados. Replicar la tabla si es necesario.

EQUIPO

CARACTERISTICA	DESCRIPCION
TIPO y FUNCION (Sobremesa, portátil, Servidor *, Nube)	
Marca	
Modelo	
Procesador	
Velocidad GHz	
Memoria RAM	
Memoria Cache	
Disco Duro	
Tipo de Monitor	

Tarjeta Grafica	
Puertos (USB, VGA, HDMI...)	
Comunicaciones (tarjeta de Red, Wifi...)	
Unidad CD y DVD(COMBO) –RW	
Controlador video	
Tipo de soporte	
Garantía	
Otras Sistemas o perifericos.	

* Indicar si es o no un servidor enracable, virtual, proveedor cloud, etc...

Indicar si existen otros dispositivos adscritos al objeto de contratación (pantallas, escáner, tablet, lectores, cámaras, etc...), que tengan o necesiten algún tipo de integración con equipamiento o infraestructura informática, incorporar una tabla con los datos específicos por cada dispositivo o en su defecto aportar las fichas técnicas en español.

OTROS DISPOSITIVOS o accesorios

CARACTERISTICA	DESCRIPCION
TIPO y FUNCION	
Marca	
Modelo	
Sistema Operativo que soporta	
Tipo de soporte	
Garantía	
Otras.....	

Adjuntar a la propuesta las fichas técnicas (Datasheet) del equipamiento.

3. CARACTERÍSTICAS SOFTWARE

Indicar si la solución propuesta requiere de algún software , características y funciones. Sistema Operativo, indicar si es Windows, Mac, Linux, así como su versión. Especificar si se trata de una versión para puesto de trabajo o servidor.

El S.O operativo debe estar actualizado y con soporte. Si no es posible su actualización continua, sino puntual, es necesario indicar la razón de ello y especificar los compromisos de actuación para su actualización.

<Insertar respuesta>

Sistema Operativo

CARACTERISTICA	DESCRIPCION
Sistema (Windows, Mac, Linux)	
Versión	
Tipo de soporte	
Garantía	

Otras.....	
------------	--

El Antimalware operativo debe estar actualizado y con soporte. Indicar la forma de actualización continua necesaria

<Insertar respuesta>

Antimalware

CARACTERISTICA	DESCRIPCION
Fabricante	
Nombre Comercial	
Versión	
Sistema Operativo que soporta	
Tipo de soporte	
Garantía	
Otras.....	

Indicar si las aplicaciones relacionadas, requiere recursos Hardware adicionales, disponen de drivers específicos que deban ser instalados.

<Insertar respuesta>

Otras aplicaciones o sistemas middleware

CARACTERISTICA	DESCRIPCION
Fabricante	
Nombre Comercial	
Versión	
Uso local o en red	
Usuarios	
Tipo y duración de la licencia	
Tipo de soporte	
Garantía	
Otras.....	

Indicar si existen posibles integraciones con otros aplicativos.

<Insertar respuesta>

Indicar si el Software tiene capacidad para realizar operativas de apoyo, respaldo en copias de seguridad, reportes y auditorías de acceso a la aplicación y datos.

<Insertar respuesta>

4. DATOS

Indicar si existe en la solución propuesta requiere algún tipo de almacenamiento de información. En caso afirmativo especificar lo siguiente:

- Tipo (carácter personal, ...)
- Ubicación y Almacenamiento (local, nube). Especificar en qué equipo reside conforme los equipos informados y el diagrama conceptual aportado.
- Capacidades de copia de respaldo.

<Insertar respuesta>

5. COMUNICACIONES

Indicar si la solución propuesta requiere de algún elemento hardware o Software de comunicaciones, o servicio de comunicaciones con algún operador e incluir sus características.

Equipos de comunicaciones

CARACTERISTICA	DESCRIPCION
Fabricante	
Marca	
Modelo	
Sistema Operativo que soporta	
Tipo de Conectividad, Red, Wifi, Otras	
Tipo de soporte	
Garantía	
Otras.....	

Sistemas Software de comunicaciones y Conexiones de red. Especificar elementos de software que faciliten las comunicaciones o que implemente seguridad y cifrado en ellas.

- Navegador, protocolos de encriptación (TLS versión o similar)
- Sistemas de seguridad en red (firewalls, IDS, WAF, etc...)

<Insertar respuesta>

Adjuntar a la propuesta las fichas técnicas (Datasheet).

6. REQUISITOS DE SEGURIDAD

Requisitos de Seguridad, debe indicarse la capacidad del proveedor para su cumplimiento y en caso contrario justificar las causas proponiendo alternativas.

Ordenadores Personales y Servidores, Puertos.

- Únicamente deben de estar habilitados los puertos (Serie, USB, HDMI...) necesarios. Por defecto, salvo justificación, no debe poderse sacarse información a dispositivos externos a través de los puertos indicados.

<Insertar respuesta>

Sistema Operativo

- El S.O debe estar actualizado de forma continua y con soporte. Si no es posible su actualización continua, y por el contrario debe ser puntual, es necesario indicar la razón de ello y programar ventanas de actuación para su actualización. La ventana máxima de actualización debe ser 3 meses por política de seguridad de FREMAP. Especificar el compromiso de actualización.

<Insertar respuesta>

- El S.O debe de tener activado el firewall y únicamente permitido el tráfico necesario para el correcto funcionamiento del aplicativo. Así mismo debe realizarse bastionado conforme el SO. Especificar medidas en este sentido por cada componente de la solución.

<Insertar respuesta>

- El S.O debe de tener habilitados / arrancados únicamente los servicios / procesos necesarios para el correcto funcionamiento del aplicativo. Responder por cada componente de la solución.

<Insertar respuesta>

Cifrado

- Las unidades de disco deben de estar cifradas en reposo, tanto unidades de almacenamiento de datos como servidores, y cualquier otra unidad que se use para traspasar los datos. Responder por cada componente y el tipo de cifrado.

- La comunicación por red y cualquier movimiento de datos entre los distintos sistemas debe estar cifrada. Responder por cada componente y el tipo de cifrado.

<Insertar respuesta>

Usuarios

- Los usuarios con acceso al equipo / aplicativo, salvo caso justificado / puntual, no deben de tener permisos de administrador sobre el equipo.

- En caso de S.O Windows, el sistema debe tener activado el control de cuentas de usuarios (UAC). En caso de otro S.O, su funcionalidad equivalente.

<Insertar respuesta>

Antivirus

- El sistema debe de disponer de un antimalware, el cual debe de estar actualizado constantemente o como máximo una actualización diaria y, configurado con las excepciones imprescindibles para el servicio.

<Insertar respuesta>

Directorio Activo

- El servidor debe de poder prestar servicio sin necesidad de incorporarse al dominio de FREMAP con Directorio Activo Microsoft. Será decisión de FREMAP, su evaluación e incorporación al mismo.

- Sería deseable que el aplicativo pudiera integrarse con Directorio Activo o ADFS en el caso de sistemas cloud, para una gestión integral de usuarios, sin necesidad de que el servidor. Especificar posibilidades.

<Insertar respuesta>

Gestión de usuarios de aplicación y contraseñas

- La aplicación deberá disponer de mecanismos de control para la asignación de los derechos de acceso, así como registro de los derechos asignados.

<Insertar respuesta>

- La aplicación deberá disponer de un registro de altas y bajas de usuarios. Presentar un ejemplo de cómo se almacena esta información.

<Insertar respuesta>

- La aplicación deberá facilitar la comunicación secreta de las credenciales de los usuarios. Especificar el procedimiento.

<Insertar respuesta>

- La aplicación deberá facilitar la revisión de los derechos de accesos por parte de los responsables FREMAP. Especificar el procedimiento.

<Insertar respuesta>

- La aplicación deberá facilitar la gestión de contraseñas por parte de los usuarios de manera que estos puedan escoger y cambiar su clave de acceso, aplicando reglas de construcción complejas que las fortalezcan. La política de creación, vigencia, bloqueo y obsolescencia de claves deberá ser la misma que la de FREMAP.

<Insertar respuesta>

- Las contraseñas deberán almacenarse encriptadas y protegidas.

<Insertar respuesta>

- Los perfiles de acceso serán definidos por el responsable de FREMAP. Especificar que capacidades por roles permite la aplicación.

<Insertar respuesta>

- La autenticación de usuarios deberá integrarse con el Directorio Activo de FREMAP o el ADFS en sistemas cloud, facilitando el Single Sign On. Especificar si es posible.

<Insertar respuesta>

Navegación a Internet

- La navegación a Internet desde los equipos y componentes queda prohibida, salvo a las direcciones necesarias para el correcto funcionamiento del aplicativo, actualización del S.O, antivirus, etc... Se debe justificar por qué es necesario la conectividad en internet y las URLs que son necesarias la conectividad.

<Insertar respuesta>

Acceso remoto

- En caso de la necesidad de acceso remoto, FREMAP cuenta con sus propios sistemas de control de acceso remoto al que el licitador se deberá de ajustar. En cualquier caso, describir las distintas alternativas para el acceso a los sistemas que se presenten. En caso de sistemas cloud, especificar como se conecta a estos sistemas el usuario final.

<Insertar respuesta>

Monitorización remota

- Algunos sistemas presentan posibilidad de monitorización remota con sistemas externos o cloud. Especificar qué tipo de conexiones y a que sistemas se realizan. Especificar como se está monitorizando la infraestructura por parte del adjudicatario.

<Insertar respuesta>

Auditoría

- El equipo debe de tener activado la auditoria para registrar, en la mayoría de lo posible, la actividad de los usuarios que acceden al sistema y la actividad dentro de la propia aplicación. 90 días es el tiempo deseable para guardar esa información.

<Insertar respuesta>

Gestión de Vulnerabilidades.

- El proveedor deberá especificar el procedimiento de identificación y gestión de vulnerabilidades que puedan afectar a la aplicación, junto con los planes de acción para su resolución.

<Insertar respuesta>

Seguridad de acceso

- En general todos los equipos deberán de tener algún mecanismo de seguridad física para poder anclarse a algún sitio, de tal forma, que no sea fácil, el robo del mismo. Si es un sistema virtual cloud, especificar los componentes, roles y reglas que securizan el acceso al sistema.

<Insertar respuesta>

Planes de backup del entorno

- El proveedor debe especificar los sistemas que intervienen para garantizar las copias de seguridad y las políticas que se siguen. Así mismo especificar la cantidad de tiempo del dato que se puede recuperar.

<Insertar respuesta>

- El Backup debe residir encriptado en sus unidades de almacenamiento. Especificar si esto es así y la criptografía usada.

<Insertar respuesta>

Planes de recuperación del entorno

- Debe existir un plan de Disaster Recovery junto con su procedimiento de backup / recuperación del entorno. El procedimiento de recuperación del entorno debe de realizarse por parte del fabricante.

<Insertar respuesta>

- Debe existir un plan de acción frente a ransomware, que incluya procedimientos para mitigar tanto el riesgo como la pérdida de la información. Aportar información detallada.

<Insertar respuesta>

Licenciamiento

- Cualquier licenciamiento de S.O, Antivirus, SW de Control remoto, etc.. Debe ser proporcionado por parte del fabricante. Aportar información de licenciamiento y periodo de renovación.

<Insertar respuesta>

7. Integración con servicios externos o de FREMAP

- Especificar si es necesario la conectividad con dispositivos de FREMAP. Incluir características, dependencias, puertos, protocolos, etc.. Especificar si hay dependencias del servicio que se ofrece con elementos no propietarios de la presente contratación.

<Insertar respuesta>

- Especificar si es necesario la conectividad con dispositivos de terceros. Incluir características, dependencias, puertos, protocolos, etc.. Especificar si hay dependencias del servicio que se ofrece con elementos no propietarios de la presente contratación.

<Insertar respuesta>

8. Prestación del Servicio.

Indicar las condiciones de servicio respecto a la garantía y mantenimiento para los equipos y aplicaciones descritos en los apartados anteriores.

<Insertar respuesta>

Incluir al menos las modalidades servicio de mantenimiento en cuanto su duración, los niveles de servicio, tipo soporte y operación periódica para el correcto funcionamiento de los equipos y aplicaciones descritos en los apartados anteriores.

<Insertar respuesta>

El servicio debe incluir los procedimientos que se siguen ante incidentes y cambios, junto con su procedimiento de comunicación y seguimiento. Especificar como son estos procedimientos (acciones ante cambios problemáticos, incidencias críticas, etc...)

<Insertar respuesta>

El licitador deberá contar con planes de revisión de capacidad y rendimiento periódicos. Especificar qué actividades comprenden y su periodicidad.

<Insertar respuesta>

Especificar cumplimiento de certificaciones externas como ISO 27001 o Esquema Nacional de Seguridad (en qué grado)

<Insertar respuesta>