

## **ANEXO V – ACCESO REMOTO A LOS EQUIPOS**

Para todos aquellos accesos remotos a recursos desplegados en FREMAP, se establecen las siguientes limitaciones y responsabilidades específicas que tanto el adjudicatario como quien actúe en su nombre, si fuera el caso, deberá cumplir:

- Condiciones técnicas:
  - La comunicación se realizará punto a punto entre las dependencias del adjudicatario y/o fabricante y FREMAP empleando un canal de datos seguro (cifrado).
  - El canal seguro se establecerá con un software específico y podrá variar en función del proveedor del sistema de terminación de túneles de FREMAP (actualmente el software referido es Cisco AnyConnect).
  - La seguridad vendrá dada por un doble factor de autenticación y podrá variar en función del proveedor elegido por FREMAP para este fin (actualmente, este proveedor es swivelsecure).
  - Actualmente, el software de generación de claves de autenticación únicamente podrá estar instalado en un dispositivo de la infraestructura propiedad del adjudicatario, proporcionando FREMAP licencia para este dispositivo.
  - El medio técnico preferente de conexión para accesos puntuales será el establecimiento de una conexión mediante VPN. Para ello, con independencia del presente clausulado, se deberá informar a FREMAP tanto de la hora de conexión como la de finalización de la sesión, así como el motivo de esta.
- Recursos de FREMAP accesibles:
  - Solamente se proporcionará acceso remoto a los elementos estrictamente necesarios para el cumplimiento del objeto contractual.
  - La conexión se realizará única y exclusivamente por unos protocolos previamente consensuados con FREMAP.
- Potestad de control
  - El personal autorizado de FREMAP, teniendo como finalidad la protección, optimización y mejora de los servicios, monitorizará el tráfico cursado en este tipo de conexiones para la detección de actuaciones anómalas.
- Deberes y obligaciones para la empresa adjudicataria:
  - Solamente deberá tener acceso a los recursos desplegados en FREMAP el personal estrictamente necesario de la empresa adjudicataria y/o fabricante y únicamente para los fines previamente autorizados por FREMAP.
  - Los usuarios del acceso remoto deberán hacer un uso adecuado de la conexión, utilizándola eficientemente con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.
- Se deberá acceder desde equipos y/o redes protegidas que garanticen unas condiciones de seguridad adecuadas sobre todo en lo referente al control de accesos al personal autorizado y la protección de los activos de FREMAP a los que se tenga acceso (lo que requiere el uso de soluciones actualizadas, antivirus, antispyware, etc....).

- El adjudicatario será responsable directo de todas las actividades realizadas mediante el uso del acceso remoto proporcionado.
- El adjudicatario deberá reportar a FREMAP aquellas incidencias de seguridad de las que tuviesen conocimiento (p.ej.: pérdida o compromiso de las credenciales, etc.).
- Uso no adecuado: el acceso remoto proporcionado no debe ser usado para:
  - Cualquier transmisión de información o acto que vaya en contra de la legislación vigente que sea de aplicación.
  - Fines privados, personales o comerciales, no relacionados con las actividades propias y autorizadas por FREMAP.
  - Transmisión de material que infrinja la legislación sobre propiedad intelectual (software, imágenes, video, audio, películas, etc.). En general la empresa adjudicataria se compromete a no hacer uso de los recursos informáticos y de comunicación para publicar o divulgar material que pueda suponer una violación de los derechos legales de terceros.
  - Creación, utilización y transmisión de cualquier tipo de material que perjudique la dinámica habitual de los usuarios de FREMAP o redes externas (virus, difusión de correo publicitario, cadenas de correo electrónico, etc.).
  - Actividades deliberadas con alguna de las siguientes finalidades:
    - Congestión de los enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
    - Escaneo de puertos.
    - Búsqueda de vulnerabilidades en equipos pertenecientes a FREMAP o redes externas.
    - Denegación de servicios y desconexión de equipos.
    - Destrucción o modificación de la información.
    - Violación de la privacidad e intimidad de los clientes de FREMAP.
    - Intentos de acceso o accesos no autorizados a equipos.

El licitador podrá optar por llevar a cabo la conexión por otros medios distintos a los especificados en las “Condiciones Técnicas” (p.ej. sesión Webex o similar), si existiera algún tipo de factor técnico u organizativo que así lo requiriese, siempre que la conexión fuera segura, que se pudiera seguir cumpliendo el resto de los puntos del presente apartado y que no supusiese ningún coste adicional para FREMAP.

NOTA: La plataforma de licitación electrónica de FREMAP únicamente permite subir un único archivo. El licitador deberá presentar los siguientes documentos en un archivo comprimido (.ZIP) o un PDF conjunto:

- Anexo I – OFERTA ECONÓMICA.
- Descripción de las condiciones técnicas propuestas para tener acceso remoto en caso de optar por llevar a cabo la conexión por otros medios distintos a los especificados en el presente Anexo, todo ello sin que suponga coste adicional para FREMAP.