

# Documentación de la dirección de tecnologías de la información

## 076 Anexo para contratos de bienes y servicios con elementos relacionados con TI

Sistemas de la Información y Ciberseguridad

**Autor: Jesús José Sola Ruiz**

**Versión: 1**

## Índice

<b>A.Condiciones generales de diseño, implantación, explotación y acceso a los sistemas de IFEMA MADRID .....</b>	<b>3</b>
Seguridad.....	3
Dimensionamiento .....	3
Pruebas de carga.....	4
Alta disponibilidad y redundancia .....	4
Conformidad con normativa de Protección de Datos .....	4
Infraestructura virtual .....	4
Inicios, apagados y reinicios consistentes automáticos .....	4
Actualizaciones .....	5
Monitorización.....	5
Copia de seguridad .....	5
Logs .....	5
Operaciones periódicas de mantenimiento de sistemas automáticas .....	6
Manual de operaciones de sistemas .....	6
Condiciones de Soporte .....	7
Autenticación y Autorizaciones de los usuarios .....	7
Confidencialidad de los datos .....	8
Devolución de servicio.....	8
Integraciones con otros productos o servicios .....	8
Tratamientos con datos de carácter especial.....	8
<b>B.Acceso a la Información.....</b>	<b>9</b>
<b>C.Seguridad en las comunicaciones y recursos de red .....</b>	<b>12</b>
<b>D.Seguridad en las estaciones de trabajo.....</b>	<b>14</b>

## **A. Condiciones generales de diseño, implantación, explotación y acceso a los sistemas de IFEMA MADRID**

Cualquier producto o servicio relacionado con los recursos informáticos de IFEMA MADRID, en adelante, solución, debe ajustarse a las condiciones generales que se describen en este apéndice.

El objeto de estas condiciones generales es obtener soluciones seguras, eficientes, sostenibles en su explotación y acordes tanto con la legislación y reglamentación vigentes como con las circunstancias y estrategias de la explotación de los Sistemas de IFEMA MADRID y asimismo conformes también con las mejores prácticas de sistemas actuales.

Todas las condiciones generales de sistemas se tendrán en cuenta desde el principio, por diseño, para evitar la introducción de retrasos de última hora. El equipo de Proyecto se reunirá con Sistemas de IFEMA MADRID en las fases iniciales del proyecto para informar de los elementos de sistemas de que consta la solución, con los datos y criterios necesarios para que el equipo de Sistemas de IFEMA MADRID pueda adoptar los compromisos y las decisiones informadas más adecuadas en materia de sistemas para IFEMA MADRID.

El presente documento también detalla todos los aspectos técnicos relacionados con la seguridad en los accesos a los recursos informáticos IFEMA MADRID.

### **Seguridad**

El diseño de la solución ofrecida y su implantación serán seguros desde el principio, se adoptarán las metodologías y paradigmas desde un enfoque de seguridad por diseño.

El proyecto activará de forma adecuada y aprovechará todas las medidas y procedimientos que ofrezcan todos los productos o servicios relacionados con el fin de incrementar la seguridad del resultado final de la implantación, de acuerdo con los requisitos y necesidades de IFEMA MADRID.

### **Dimensionamiento**

El dimensionamiento, la parametrización y la asignación de recursos de los productos o servicios que integren el proyecto tendrán en cuenta la actividad esperada y las condiciones particulares del proyecto. Se propondrán valores para conseguir un rendimiento y tiempos de respuesta adecuados si incurrir en excesos en la asignación de recursos que no se vayan a aprovechar. La capacidad asignada a los recursos deberá cubrir las necesidades previstas para un período razonable y sin desaprovechar. Por ejemplo, para cubrir las necesidades de un año u otro período que se especifique para el producto o servicio en particular.

## **Pruebas de carga**

Antes del primer uso productivo de las soluciones ofrecidas se realizarán las pruebas de carga simulando la actividad máxima esperada. Con objeto de comprobar que la solución implantada ofrece los tiempos de respuesta adecuados para un sistema productivo y que el consumo de recursos es acorde a la capacidad de la infraestructura asignada.

## **Alta disponibilidad y redundancia**

Las ofertas de soluciones críticas para el negocio de IFEMA MADRID cuya indisponibilidad pueda ocasionar un impacto elevado estarán dotadas de medidas de alta disponibilidad y de redundancia adecuadas. En la fase de comprobaciones del proyecto de implantación se comprobará el funcionamiento correcto de todas estas medidas de alta disponibilidad y redundancia. A conveniencia de IFEMA MADRID podrían pactarse otras condiciones de disponibilidad.

## **Conformidad con normativa de Protección de Datos**

El resultado del proyecto y sus productos serán conformes a la normativa legal vigente dando cumplimiento a las directivas, leyes y reglamentos en vigor, así como a las normas internas de IFEMA MADRID.

Los datos, tratamientos, diseños y toda la información que pertenece a IFEMA MADRID son confidenciales y deben protegerse con la máxima diligencia. Todos estos elementos, en el caso de una solución "Cloud" o SaaS de software como servicio, deben estar siempre físicamente ubicados en servidores, sistemas y centros de proceso de datos que dispongan de las máximas garantías respecto a medidas de seguridad y deben estar ubicados dentro del territorio perteneciente a la Unión Europea. En tanto en cuanto se utilicen medidas que garanticen la confidencialidad de los datos, las personas autorizadas podrán acceder a los sistemas y datos de IFEMA MADRID independientemente de la ubicación en que se encuentren dichas personas. Estos accesos no deben quedar al alcance de personas no autorizadas. Por ejemplo, los accesos en general y los accesos desde fuera de la Unión Europea en particular se efectuarán a través de canales seguros, cifrados y autenticados.

## **Infraestructura virtual**

Todas las soluciones ofrecidas para una solución "On Premise" deberán funcionar apropiadamente en el entorno de virtualización VMWare vSphere en su versión 6 actual disponible en IFEMA MADRID y en sus versiones posteriores, según se modernice.

## **Inicios, apagados y reinicios consistentes automáticos**

Las soluciones diseñadas para funcionar en los propios sistemas de IFEMA MADRID se integrarán automáticamente y sin requerir la intervención de persona alguna con las operaciones de inicio, apagado y reinicio de dichos sistemas en los que funcionan. Todas estas operaciones mantendrán la consistencia de los datos. El apagado del sistema operativo consolidará de forma consistente todos los datos de la solución antes de detenerla. El encendido del sistema operativo también

arrancará automáticamente todos los productos de la solución hasta el estado normal para dar servicio a los usuarios, sin requerir la intervención de ninguna persona.

## Actualizaciones

Todas las soluciones ofrecidas dispondrán como mínimo de actualizaciones de seguridad, actualizaciones para resolver errores, para adaptarse a los cambios en las normativas legales, etc.

La implantación inicial de las soluciones ofrecidas se hará con sus últimas versiones y actualizadas hasta los niveles más modernos disponibles.

## Monitorización

Las situaciones durante la explotación de las soluciones ofrecidas que requieran la atención de personas de Sistemas de IFEMA MADRID, producirán alertas adecuadas en seguida, dirigidas a las personas responsables con información suficiente para proceder a su remedio. Por ejemplo, las soluciones ofrecidas enviarán emails a las direcciones que se indiquen durante dichas situaciones.

## Copia de seguridad

Para las soluciones "On Premise", se activarán los mecanismos para obtener copias de seguridad eficientes y consistentes de la solución y sus datos con el producto Veeam Backup 9.5 disponible actualmente en IFEMA MADRID y con sus versiones más modernas, según se vaya actualizando. Se documentarán y comprobarán, de acuerdo con IFEMA MADRID, los procedimientos para recuperar de forma consistente desde datos unitarios individuales hasta la solución completa con todos sus datos, pasando por recuperaciones de conjuntos parciales de los datos necesarias para resolver los diferentes tipos de desastres posibles y minimizando las interrupciones totales del servicio en los casos de recuperaciones parciales.

Para las soluciones "Cloud". El volumen de datos en riesgo de pérdida que se considera aceptable (RPO) es el de 24 horas. El tiempo que se puede tolerar la caída de servicio por recuperación de datos (RTO) es de 24 horas.

También para soluciones "Cloud" se proporcionará el mecanismo que garantice la disponibilidad de los datos de IFEMA MADRID para IFEMA MADRID ante un cese súbito y permanente de la prestación del servicio por parte del adjudicatario.

## Logs

La generación de logs será la adecuada para un sistema productivo. Los logs se rotarán, comprimirán o borrarán con antelación suficiente a que puedan ocasionar un incidente por agotar todo el espacio disponible en el sistema productivo. No se dejará activado permanentemente ningún modo de depuración o "debug" en el sistema productivo. Los logs no contendrán información con datos sensibles o protegidos, de modo que no sean posibles incidentes de confidencialidad al investigar los logs.

## **Operaciones periódicas de mantenimiento de sistemas automáticas**

Las operaciones periódicas rutinarias de mantenimiento de sistemas se entregarán automatizadas. Operaciones tales como búsqueda y borrado de elementos temporales, reindexaciones de contenidos, optimizaciones de funcionamiento, optimizaciones de datos, etc. Todas estas operaciones rutinarias se realizarán periódicamente de forma desatendida y por las noches, fuera del horario productivo, para evitar impacto en disponibilidad y en tiempos de respuesta.

Otras operaciones de sistemas que implican impacto o riesgo en la disponibilidad o integridad del servicio productivo, no serán automáticas porque no son en absoluto rutinarias. Estas operaciones se documentarán bien para que el equipo de Sistemas de IFEMA MADRID las planifique y las lleve a cabo, en su caso, en el momento más oportuno. Operaciones tales como las actualizaciones de software, por ejemplo.

## **Manual de operaciones de sistemas**

Se entregará con la solución el manual de operaciones de sistemas habituales para el producto. Se hará hincapié en la elaboración de procedimientos precisos para aquellas operaciones de sistemas que sean industrializables y frecuentes, para que las puedan llevar a cabo equipos de Sistemas no especializados de primer nivel o de atención al usuario.

Determinar el estado del servicio o producto, en particular su estado de disponibilidad.

Alta y baja de nuevos usuarios en el producto. Cambios de departamento o de las funciones de usuarios existentes, etc.

Desbloqueo de identificadores de usuarios. Resolución de olvidos de contraseñas.

Cualquier otra operación específica del producto, servicio o solución que sea frecuente, se documentará de forma precisa para que la lleve a cabo personal menos especializado.

Se documentarán también las operaciones de sistemas de segundo nivel. Entre ellas, por ejemplo:

Procedimientos de apagado consistente y arranque integrados con el apagado e inicio del sistema operativo

Investigación de incidentes: apertura de casos en el soporte oficial, priorización de incidentes, escalado de incidentes, obtención y envío de datos de los logs al soporte oficial.

Operaciones periódicas de mantenimiento no rutinarias, por ejemplo, aplicación de actualizaciones

Ajustes en la configuración de los servicios, optimización de recursos, parametrización, etc.

Mantenimiento de las interfaces de los productos de la solución entre sí como de las interfaces con otros productos. Por ejemplo, documentar la ubicación de elementos que pueden cambiar con la evolución de las infraestructuras tales como los datos de

credenciales o conexión IP y puerto del driver de una base de datos o de la interfaz a un servicio RFC, cambios en la URL de un webservice, cambios de elementos de seguridad, de elementos de autenticación con otros productos (básica, integrada, single-sign-on, certificado digital, etc.)

## **Condiciones de Soporte**

Las soluciones ofrecidas contarán con soporte específico de sistemas. En el caso de soluciones que sean críticas para el negocio de IFEMA MADRID será 24x7x365 en castellano y con tiempos de respuesta de menos de una hora ante incidentes graves (24 horas al día, 7 días por semana, todos los días del año). De lo contrario, a conveniencia de IFEMA MADRID, se podrían pactar condiciones de soporte diferentes. Por ejemplo: para soluciones no críticas el soporte podría ser 14x7x365, en horario laboral de IFEMA MADRID, con tiempo de respuesta de menos de una hora ante incidentes graves.

## **Autenticación y Autorizaciones de los usuarios**

La solución incluirá el diseño y la implantación de las autorizaciones para los usuarios de los productos o servicios. Tendrá en cuenta las obligaciones y las atribuciones de los diferentes usuarios que la emplearán: se permitirá a cada tipo de usuario ejecutar sólo lo necesario sobre los datos que le correspondan y se impedirá que puedan realizar las actividades no necesarias y acceder a los datos que no les correspondan.

De los mecanismos de autenticación y autorización disponibles se optará por el que esté integrado con el Directorio Activo (DA) de Microsoft de IFEMA MADRID. Caso que no exista integración con DA, se optará por el mecanismo más seguro entre los disponibles, de acuerdo con los requisitos e indicaciones de IFEMA MADRID.

Los sistemas de autenticación básica basados en contraseñas deben tener las medidas que impiden que se adivinen o desvelen a personas no autorizadas. Por ejemplo, políticas que obliguen escogerlas con complejidad adecuada de longitud, letras, cifras y símbolos. Contraseñas que fueren renovación periódica, con periodos de validez y caducidad automática. Contraseñas que no se encuentren ni en los diccionarios ni en las listas de contraseñas frecuentes. Estos sistemas tendrán protección contra los ataques de fuerza bruta bloqueando los intentos fallidos de acceso repetidos.

En las soluciones en "Cloud" las credenciales de autenticación deben viajar por canales cifrados seguros https / TLS. Son imprescindibles todas las medidas de fortaleza de contraseñas descritas así como las medidas de seguridad adicionales presentes en los productos ofrecidos.

En ningún caso se dejarán contraseñas por defecto a los identificadores de usuario predefinidos de los productos de la solución.

El acceso a los datos sensibles de IFEMA MADRID requiere las medidas de autenticación más seguras, por ejemplo, la autenticación de dos factores. Sin perjuicio de las medidas adicionales para el tratamiento de datos sensibles en general que se describen en su propio apartado más adelante.

## **Confidencialidad de los datos**

Los datos de la solución ofrecida no estarán disponibles para las personas no autorizadas. En todo momento los datos estarán protegidos por las medidas de seguridad de la solución ofrecida.

Para el caso de soluciones con tratamientos o datos confidenciales o sensibles en "Cloud", la solución dispondrá de medidas técnicas que garanticen que los datos confidenciales o sensibles no pueden accederse ni siquiera por los administradores de sistemas de la solución ni por los del servicio de alojamiento o hosting empleado.

## **Devolución de servicio**

Para soluciones basadas en servicios, en caso de finalizar el servicio, es necesario ejecutar la fase de devolución del servicio a IFEMA MADRID. El proveedor deberá devolver todo lo necesario a IFEMA MADRID para poder continuar con el servicio en otro proveedor "Cloud" u "On Premise", en el formato y forma que IFEMA MADRID decida. Se emplearán los formatos estándar de intercambio de datos para los tipos de elementos que se trate. Por ejemplo, se incluirán todos los datos, toda la documentación del servicio, de procedimientos, de medidas de seguridad, de integración con otros productos o servicios, etc

Durante la fase de devolución del servicio, el proveedor del contrato que finaliza colaborará plenamente con el nuevo prestador del servicio con objeto de lograr una transición íntegra, rápida y segura de todos los elementos que consta el servicio. La fase de devolución del servicio es una de las fases incluidas en la propia solución.

## **Integraciones con otros productos o servicios**

Las integraciones de la solución con otros productos o servicios se realizará de forma totalmente segura, tal y como corresponde al diseño de la solución, para conseguir una integración invulnerable. Por ejemplo, las comunicaciones entre diferentes productos irán autenticadas, firmadas y cifradas entre ambos extremos.

Las integraciones serán resistentes y a indisponibilidades en cualquiera de los extremos y se repondrán automáticamente. Por ejemplo, si uno de los extremos se hallase indisponible temporalmente por mantenimiento o por contingencia, en cuanto vuelva a estar disponible, la integración entre ambos extremos se debe reanudar automáticamente, sin intervención de las personas, de un modo consistente con el tratamiento y con los datos de ambos extremos.

## **Tratamientos con datos de carácter especial**

En relación con los datos de carácter especial debido a su incidencia en la intimidad, las libertades públicas y los derechos fundamentales de las personas tales por ejemplo como los datos de menores de edad, de personas vulnerables, genéticos, biométricos, de salud, de origen étnico, de afiliación sindical, convicciones religiosas, etc. o cualesquiera otros datos que la reglamentación vigente considere como dato de carácter especial.

Si el contratante debe acceder a datos como los descritos o si la solución que va a instalar implica el tratamiento de este tipo de datos, entonces, con el fin de garantizar un nivel de seguridad adecuado al riesgo, se deben incorporar obligatoriamente, al menos, dos de las siguientes medidas de seguridad técnica, sin perjuicio de otras medidas más estrictas y específicas exigidas en otras partes de este contrato:

- a) la seudonimización y el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento

## **B. Acceso a la Información**

En el caso en que la solución conste de acceso a la información o a los tratamientos de IFEMA MADRID, dicho acceso está autorizado únicamente a los recursos dentro de los objetivos y alcance de este contrato. Además dicho acceso estará sujeto a las condiciones que se describen a continuación.

No están permitidos otros accesos que se encuentren fuera de los objetivos y alcance de este contrato.

El adjudicatario deberá implementar los mecanismos de seguridad necesarios para garantizar la seguridad, confidencialidad y disponibilidad de las soluciones: datos, tratamientos, sistemas, productos, servicios, etc.

El adjudicatario respetará las disposiciones legales reglamentarias y normativas vigentes, incluyendo la normativa de seguridad de la información de IFEMA MADRID y su Política de Seguridad.

IFEMA MADRID entregará al adjudicatario el documento de normativa interna, perteneciente a la Política de Seguridad de IFEMA MADRID, llamado "Normas del Personal externo con acceso a los sistemas" que será de obligado cumplimiento por todos los usuarios que requieran algún tipo de acceso a los sistemas, tratamientos o datos de IFEMA MADRID, tanto de forma remota como presencial.

- Sólo aquellos empleados del adjudicatario debidamente autorizados en razón del servicio podrán acceder a los tratamientos o sistemas informáticos de IFEMA MADRID y sólo desde aquellos puestos (terminales) y emplazamientos debidamente autorizados, y sólo a los recursos, tratamientos e información autorizados por IFEMA MADRID.
- El adjudicatario informará de cualquier cambio de su personal con autorización de acceso a los tratamientos o sistemas informáticos de IFEMA MADRID con tiempo suficiente para la revocación/autorización de sus accesos. El adjudicatario auditará y controlará quien accede, en qué momento y con qué objetivo a los sistemas y datos de IFEMA MADRID e IFEMA MADRID debe conocer en un momento dado quiénes son las personas concretas que

acceden. No están permitidos ni los accesos no justificados ni los accesos por personas desconocidas.

- IFEMA MADRID podrá monitorizar cualquier acceso a sus tratamientos y sistemas de información. Se asumirá que los actos que se lleven a cabo con el identificador y la clave de acceso asignados han sido realizados en realidad por el usuario titular de los mismos. Siempre se hará buen uso del identificador de usuario asignado y se custodiará con eficacia la clave de acceso personal. Las autorizaciones de acceso a los tratamientos de IFEMA MADRID son personales e intransferibles, por tanto, el personal del adjudicatario no podrá ceder sus cuentas ni claves de acceso a otras personas.
- El adjudicatario pondrá todos los medios técnicos y adoptarán todas las medidas de seguridad necesarias para garantizar que sólo podrán acceder a los tratamientos, recursos y sistemas de IFEMA MADRID únicamente aquellas personas autorizadas para la prestación de la solución objeto de este contrato, sin que haya intromisión de otros recursos y soluciones que el adjudicatario pudiese prestar a terceros.
- El uso por parte de los empleados del adjudicatario de los tratamientos o de los sistemas informáticos de IFEMA MADRID estará restringido al horario de servicio. Al finalizar, todos los usuarios deberán realizar el procedimiento de salida de las aplicaciones y la desconexión de la red de IFEMA MADRID. Cualquier ampliación del horario del servicio sólo podrá ser autorizado por IFEMA MADRID previa solicitud escrita a su responsable.
- Siempre que el adjudicatario esté en relación con el tratamiento de datos de carácter personal, en su calidad de encargado de tratamiento, para la prestación del servicio objeto del contrato, conoce y acepta que todo su personal que preste servicio a IFEMA MADRID estará informado de los términos y condiciones establecidas en relación con el citado tratamiento de datos, así como la legislación vigente de protección de datos de carácter personal de obligado cumplimiento. En este sentido, todo el personal que preste servicio a IFEMA MADRID deberá firmar el correspondiente Acuerdo de Confidencialidad y recibirá unas las Normas de Uso de Sistemas de IFEMA MADRID.
- No se intentará descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en el acceso lógico a los sistemas informáticos de IFEMA MADRID. No está permitido acceder a los recursos de IFEMA MADRID no autorizados expresamente por IFEMA MADRID. Se accederá únicamente a los recursos, datos, servicios y aplicaciones autorizadas.
- El uso de los recursos informáticos de IFEMA MADRID se ajustará a lo estipulado en las presentes condiciones y únicamente con el propósito de acometer exclusivamente los fines y objetivos de IFEMA MADRID.
- No deberán imprimirse en papel, grabarse ni obtener copias de los datos procedentes de IFEMA MADRID en ningún dispositivo de almacenamiento incluyendo los discos duros de los equipos empleados; salvo que sea necesidad para los usos previstos y autorizados para la prestación del servicio.

- Cualquier incidencia o brecha de seguridad deberá ser notificada a IFEMA MADRID.
- Ningún usuario deberá poseer, para usos no propios de su responsabilidad u objeto del contrato, material o información alguna propiedad de IFEMA MADRID, tanto ahora como en el futuro.
- Todos los recursos informáticos disponibles, son propiedad de IFEMA MADRID y no deberán ser accedidos ni visualizados por personas no autorizadas en las pantallas de los equipos empleados. El usuario deberá custodiar también los documentos o listados que imprima con datos procedentes de la red corporativa de IFEMA MADRID.
- En el caso de que, por motivos directamente relacionados con el servicio a prestar, el usuario entre en posesión de datos de carácter personal o información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le conceda derecho alguno de posesión, titularidad o copia sobre la referida información. Asimismo, el usuario deberá devolver dichos materiales a IFEMA MADRID, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral o contractual. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de IFEMA MADRID, no supondrá, en ningún caso, una modificación de esta cláusula.
- Los tratamiento de datos personales a los que pueda tener acceso el adjudicatario son responsabilidad de IFEMA MADRID quien manifiesta haber dado cumplimiento a todas las obligaciones legales que con respecto a tratamientos automatizados y no automatizados que contengan datos de carácter personal, todo ello de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos o RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como las posteriores normas nacionales que puedan desarrollar esta materia.
- El adjudicatario se compromete a no revelar ni difundir a terceros los datos a los que pueda tener acceso en relación y/o como consecuencia del cumplimiento y/o desarrollo del citado servicio, los cuales tendrán en todo momento el carácter de privados y confidenciales comprometiéndose a utilizarlos únicamente conforme a las condiciones pactadas en el presente contrato, quedando expresamente prohibida cualquier comunicación de los mismos a otras personas.
- Los usuarios de los sistemas de información de IFEMA MADRID deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral o contractual con IFEMA MADRID, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato o de la relación laboral o la prestación del servicio.

- Llegado el vencimiento del contrato o finalizado cada servicio encomendado, el adjudicatario borrará totalmente de sus sistemas informáticos los datos de IFEMA MADRID sin necesidad de previo requerimiento.
- El adjudicatario conoce y acepta que cualquier otra utilización de los citados datos, o cesión de los mismos a terceros, sean o no filiales o empresas participadas por esta, para cualquier fin diferente del reseñado, constituye una vulneración del presente acuerdo de confidencialidad y de la normativa vigente de protección de datos de carácter personal declinando IFEMA MADRID cualquier responsabilidad al respecto.
- IFEMA MADRID se reserva el derecho a poder efectuar, en cualquier momento, los controles que estime oportunos para comprobar el cumplimiento de lo establecido en el presente acuerdo.
- En caso de incumplimiento de estas condiciones, el adjudicatario acepta y asume, expresamente, su plena responsabilidad, ante la Administración y/o ante terceros, respondiendo de las infracciones cometidas en relación con las disposiciones recogidas en la normativa de protección de datos de carácter personal vigente en cada momento, así como de las sanciones y/o indemnizaciones debidas a terceros, incluida IFEMA MADRID, por consecuencia de ese incumplimiento.

## **C. Seguridad en las comunicaciones y recursos de red**

En el caso en que la solución conste de interconexión con IFEMA MADRID, dicha interconexión no deberá plantear ningún riesgo para IFEMA MADRID, dispondrá de las medidas necesarias para resolver las amenazas de seguridad y tendrá la disponibilidad adecuada que requiera la solución.

- El adjudicatario deberá disponer de la infraestructura de conectividad necesaria para materializar las comunicaciones necesarias para la prestación del servicio. Dispondrá de los elementos físicos y lógicos adicionales necesarios para garantizar la seguridad en la comunicación tanto con las máquinas como con los aplicativos, utilidades y servicios implicados en las actividades de IFEMA MADRID; se compromete además a cumplir los estándares de comunicación en que se basa la arquitectura de red de IFEMA MADRID, por ejemplo adaptándose a la configuración de los elementos de seguridad tales como firewalls, proxys, etc. de IFEMA MADRID.
- El modo de comunicación debe ser ágil y seguro usando para ello las distintas posibilidades adecuadas para cada caso. Por ejemplo, entre otras, VPNs LAN to LAN, línea dedicada, etc. Se estudiarán las ofertas más ventajosas para IFEMA MADRID por parte del adjudicatario.
- Cuando dentro del alcance del contrato se encuentre establecer conectividad para la prestación del servicio, la preparación de la misma se hará justo a continuación de la formalización del contrato. El adjudicatario deberá definir los parámetros para la conexión

y llevará a cabo todas las tareas necesarias para que la conectividad esté plenamente operativa y comprobada para poder iniciar la prestación del servicio. Durante la prestación del servicio, el adjudicatario deberá además proporcionar el soporte técnico necesario para un correcto funcionamiento de las comunicaciones entre las dependencias desde las que el equipo realice los servicios durante toda la duración de la misma. Para ello debe ponerse en contacto con la Dirección de la Tecnología de la Información de IFEMA MADRID

- Cuando en el contrato se establezcan Acuerdos de Nivel de Servicio (ANS) relacionados con las comunicaciones, el adjudicatario es responsable del cumplimiento de los mismos.
- La instalación y el mantenimiento del servicio de comunicaciones correrán por cuenta del adjudicatario, por lo tanto, será el responsable tanto de la instalación, mantenimiento y costes de la infraestructura y componentes de comunicaciones, por tanto debe implementar y gestionar todo el equipamiento necesario para garantizar el correcto funcionamiento de estas comunicaciones.
- El adjudicatario proveerá infraestructura de comunicaciones de voz cuando aplique, a través preferiblemente de la interconexión de sus servicios con los de IFEMA MADRID o propuestas alternativas que garanticen las comunicaciones entre las instalaciones del proveedor y las de IFEMA MADRID, para el óptimo desarrollo del servicio.
- El adjudicatario debe aislar las conexiones para la solución, de forma que solo se puedan acceder a las mismas desde los equipos desde los que se preste servicio a IFEMA MADRID.
- Las líneas de comunicaciones de voz y datos, deberán ser escalables y que por tanto permitan aumentar el ancho de banda de forma rápida y sencilla, de acuerdo a las necesidades.
- Cuando se precisen realizar tareas desde las instalaciones del adjudicatario debido a la naturaleza del servicio, este deberá proveer Conexión a Internet propia y gestionada por él mismo para sus operadores, con un ancho de banda suficiente para garantizar el nivel de servicio, incluyendo líneas de respaldo (backup) en alta disponibilidad.
- Cuando el adjudicatario se conecte a IFEMA MADRID a través de su red corporativa facilitará plano de red con máximo nivel de detalle para validar que dicha conexión cumple con los requisitos de seguridad requeridos por IFEMA MADRID.
- Estos requerimientos técnicos pueden ser modificados por IFEMA MADRID por necesidades de negocio o técnicas y ningún cambio puede ser abordado por el adjudicatario sin consentimiento de IFEMA MADRID.

## D. Seguridad en las estaciones de trabajo

En el caso en que la solución requiera que el adjudicatario emplee sus propias estaciones de trabajo o en cualquier caso que se empleen estaciones de trabajo que no son de IFEMA MADRID, es necesario que dichas estaciones no planteen ningún riesgo para IFEMA MADRID, que dispongan de las medidas necesarias para resolver las amenazas de seguridad y seguir todos los procedimientos para el uso seguro de estaciones de trabajo, como los que se describen a continuación.

- Cuando el objeto del servicio requiera que el adjudicatario tiene que prestar el mismo desde su propia plataforma tecnológica, el adjudicatario se compromete a proporcionar una plataforma tecnológica que soporte los sistemas y herramientas utilizados, tanto propios como de IFEMA MADRID y garantice el funcionamiento del servicio y el cumplimiento de los acuerdos sobre el mismo consensuados con IFEMA MADRID. El adjudicatario deberá soportar la posible instalación de aplicaciones cliente-servidor, que pudieran ser utilizadas en función de cómo decida implementar IFEMA MADRID el acceso por los operadores.
- En todo momento el adjudicatario deberá seguir las instrucciones que IFEMA MADRID le solicite respecto de la actualización de las condiciones técnicas de los puestos de trabajo.
- Las estaciones de trabajo y dispositivos que disponga el adjudicatario para la prestación del servicio, deben cumplir con todos los requisitos de seguridad que garanticen que los recursos de IFEMA MADRID a los que acceden no sean dañados. Estos requisitos pasan por mantener un antivirus con motor y fichero de firmas actualizado y un nivel de parches de seguridad de sistema operativo actualizado con la última versión que no permitan explotar bugs, vulnerabilidades del sistema e infectarse con virus o malware. Además deberá tener activo y correctamente configurado un firewall que proteja las estaciones de trabajo.
- El adjudicatario deberá garantizar que dentro de sus instalaciones no se puedan manipular la configuración de los equipos destinados al servicio destinado para IFEMA MADRID por personal no autorizado.
- Cuando el usuario abandone su puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los tratamientos o datos protegidos.
- Cada ordenador dispondrá de un protector de pantalla con contraseña que se activará a los diez minutos de inactividad y no estará permitido desactivarlo.
- En el caso de las impresoras, el usuario deberá asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos. En las impresoras compartidas con otros usuarios no autorizados para acceder a los datos de los ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

**Dirección de tecnologías de la información**

076 Anexo para contratos de bienes y servicios con elementos relacionados con TI

- Cuando los requisitos del contrato lo requieran, el adjudicatario estará obligado a dotar la solución de los equipos informáticos necesarios para el mejor desarrollo de su función, incluyendo, los equipos (PCs, impresoras, periféricos, etc.), y los programas de software correspondientes, así como los servicios de comunicaciones que se precisen para su conexión a Internet, correo electrónico, y cualesquiera otros que interesen al servicio, asumiendo el adjudicatario los costes que estos originen. Será igualmente responsable de su mantenimiento y copias de seguridad.
- Si el objeto de la solución lo requiere, IFEMA MADRID puede proporcionar al adjudicatario dispositivos de acceso seguros, siendo estos dispositivos personales e intransferibles y que deben ser custodiados, responsabilizándose al adjudicatario de su pérdida o uso indebido por terceras personas. Una vez finalizado el servicio, el adjudicatario deberá devolver dicho dispositivo.
- Si el objeto de la solución lo requiere, IFEMA MADRID puede proporcionar software de acceso seguro a los sistemas informáticos, siendo este software de uso personal e intransferible, debiéndose eliminar a la finalización del servicio.