

ANEXO II

(Este anexo relleno por el licitador se deberá incluir en el Sobre o archivo electrónico nº 1)

MODELO DE DECLARACIÓN RESPONSABLE -

Frente a IFEMA y dentro del procedimiento de licitación del contrato, Don, con D.N.I. núm., mayor de edad, en nombre propio (o en representación de la empresa, con C.I.F. núm., y domicilio en, calle, núm.),

DECLARA BAJO SU RESPONSABILIDAD:

1. Que la licitadora está válidamente constituida y que conforme a su objeto social puede presentarse a la licitación, así como que el firmante de la declaración ostenta la debida representación para la presentación de la proposición y de aquella.

2. Que la licitadora cuenta con la correspondiente clasificación, en su caso, o que cumple los requisitos de solvencia económica, financiera y técnica o profesional exigidos, en las condiciones que establezca el Pliego de Cláusulas Administrativas Particulares.

3. Que la licitadora a la que representa legalmente, sus administradores y representantes, así como el firmante, no están incurso en ninguna de las prohibiciones de contratar contenidas en el artículo 71 de La Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. Según lo previsto en el artículo 73 de la LCSP, ni por sí misma ni por extensión, como consecuencia de la aplicación del artículo 71.3 de la LCSP.

4. Que designa como dirección de correo electrónico en que efectuar las notificaciones....., que tiene el carácter de «habilitada» de conformidad con lo dispuesto en la D.A. 15ª de la LCSP, (solo para aquellos casos en los que el órgano de contratación haya optado por realizar las notificaciones a través de la misma lo que se hará constar en el Apartado 6 del Cuadro de Características).

5. Que en la fecha en que finaliza el plazo de presentación de proposiciones u ofertas, cumple las condiciones establecidas legalmente para contratar con la Administración y en concreto las que se citan en la cláusula 19 del Pliego tipo de cláusulas administrativas particulares, aprobado por el Órgano de Contratación, dispone de la documentación que así lo acredita y se compromete a mantener dichas condiciones durante el tiempo necesario a los efectos del presente contrato.

6.- Que las copias y documentos escaneados que se presentan son copia fiel y exacta de la documentación original, y que se compromete a aportar la documentación original en cualquier momento en que sea requerido por la Comisión de Compras y Contratación o por el Órgano de Contratación.

....., de de 2020

Fdo.:
(Firma y sello de la empresa)

ANEXO III

(Este anexo relleno por el licitador se deberá incluir en el Sobre o archivo electrónico nº 1)

DATOS DE CONTACTO DEL OFERTANTE

Frente a IFEMA y dentro del procedimiento de licitación del contrato, Don, con D.N.I. núm., mayor de edad, en nombre propio (o en representación de la empresa, con C.I.F. núm., y domicilio en, calle, núm.), con la finalidad de facilitar el contacto entre IFEMA y las empresas participantes, cumplimenta la ficha incluida a continuación con todos aquellos datos de contacto profesional de las personas que intervengan en cualquier asunto administrativo/técnico relacionado con este concurso.

DENOMINACIÓN SOCIAL:	
DIRECCIÓN:	
PERSONA/S DE CONTACTO PARA ESTE EXPEDIENTE:	
TELÉFONO/S:	
FAX/ES:	
CORREO ELECTRÓNICO DE LAS PERSONA/S DE CONTACTO PARA ESTE EXPEDIENTE:	
OTROS DATOS QUE ESTIMEN DE INTERÉS:	
¿CONSIENTE QUE IFEMA CONSERVE ESTOS DATOS PARA FUTURAS LICITACIONES?	SI NO

En, de de 2020

Fdo.:

(Firma y sello de la empresa)

En cumplimiento de la normativa vigente en materia de protección de datos, le informamos de lo siguiente respecto al tratamiento de sus datos personales: Responsable: IFEMA – Feria de Madrid (Q/2873018B). Finalidad: gestionar el expediente de licitación en el que participa. Legitimación: consentimiento del interesado y relación precontactual. Destinatarios: IFEMA no comunicará los datos personales tratados a ningún tercero, salvo exigencia legal. Conservación: sus datos serán conservados hasta que se resuelva el expediente de licitación siendo suprimidos posteriormente salvo consentimiento expreso manifestado en el formulario. En ese caso se le incluirá como posible proveedor de IFEMA en el sector correspondiente a su actividad profesional. Derechos: acceder, rectificar, suprimir, limitar u oponerse al tratamiento, solicitar la portabilidad dirigiendo comunicación a Avda. del Partenón, 5 (28042) de Madrid, o por email a "protecciondedatos@ifema.es" indicando en el asunto: "Ejercicio Derechos Proveedores Licitaciones", nombre y núm. DNI. Puede recabar la tutela de la AEPD en su página web www.aepd.es y consultar nuestra política de privacidad en www.ifema.es.

ANEXO IV

(En caso de que la garantía provisional se constituya mediante aval bancario, se deberá seguir este modelo, y el documento correspondiente se deberá incluir en el Sobre o archivo electrónico nº 1)

MODELO DE AVAL BANCARIO PARA GARANTÍA PROVISIONAL

La Entidad, NIF, con domicilio en, en la calle/plaza/avenida, C.P., y en su nombre con poderes suficientes para obligarle en este acto.

AVALA

a, NIF, en concepto de garantía provisional, para responder de las obligaciones derivadas de la participación en la licitación del “.....EXP.-” ante la INSTITUCIÓN Ferial DE MADRID (IFEMA), por importe de euros (.....€).

La entidad avalista declara bajo su responsabilidad, que cumple con los requisitos previstos en el art. 56.2 del Reglamento General de Contratos de las Administraciones Públicas.

Este Aval se otorga solidariamente con respecto al obligado principal, con renuncia expresa a los beneficios de orden, división y excusión y con compromiso de pago al primer requerimiento de la INSTITUCIÓN Ferial DE MADRID (IFEMA), incluso con la oposición del afianzado y sin poder posponer el pago o negarse al mismo, por ningún motivo

El presente Aval estará en vigor hasta que se autorice su cancelación o devolución por la INSTITUCIÓN Ferial DE MADRID (IFEMA).

El presente aval se ha sido inscrito en esta misma fecha en el Registro de Avals con el número

(Lugar y fecha)

(Razón social de la Entidad)

(Firma de los apoderados)

ANEXO V

(En caso de que la garantía definitiva se constituya mediante aval bancario, se deberá seguir este modelo, y el documento correspondiente se deberá aportar en el momento que se requiera al licitador que ha presentado la mejor oferta según la cláusula 19 del Pliego de Cláusulas Administrativas Particulares)

MODELO DE AVAL BANCARIO PARA GARANTÍA DEFINITIVA

La Entidad, NIF, con domicilio en, en la calle/plaza/avenida, C. P., y en su nombre con poderes suficientes para obligarle en este acto.

AVALA

a, NIF, en concepto de garantía definitiva, para responder de las obligaciones derivadas de la adjudicación del **EXP.-** ante la INSTITUCIÓN FERIAL DE MADRID (IFEMA), por importe de euros (.....€).

La entidad avalista declara bajo su responsabilidad, que cumple con los requisitos previstos en el art. 56.2 del Reglamento General de Contratos de las Administraciones Públicas.

Este Aval se otorga solidariamente con respecto al obligado principal, con renuncia expresa a los beneficios de orden, división y excusión y con compromiso de pago al primer requerimiento de la INSTITUCIÓN FERIAL DE MADRID (IFEMA), incluso con la oposición del afianzado y sin poder posponer el pago o negarse al mismo, por ningún motivo

El presente Aval estará en vigor hasta que se autorice su cancelación o devolución por la INSTITUCIÓN FERIAL DE MADRID (IFEMA).

El presente aval ha sido inscrito en esta misma fecha en el Registro de Avaluos con el número

(Lugar y fecha)

(Razón social de la Entidad)

(Firma de los apoderados)

ANEXO VI

(En caso de que la garantía provisional se constituya mediante seguro de caución, se deberá seguir este modelo, y el documento correspondiente se deberá incluir en el Sobre o archivo electrónico nº 1)

MODELO DE CERTIFICADO DE SEGURO DE CAUCIÓN

Certificado número(1)(en adelante, asegurador), con domicilio en....., calle....., y NIF....., debidamente representado por Don(2), con poderes suficientes para obligarle en este acto.

ASEGURA a(3), NIF....., en concepto de tomador del seguro, ante la INSTITUCIÓN FERIAL DE MADRID (IFEMA), en adelante asegurado, hasta el importe de(en letras y en cifras), en los términos y condiciones establecidos en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, las Instrucciones Internas de Contratación de IFEMA, la normativa de desarrollo y el Pliego de Cláusulas Administrativas Particulares por los que se rige el **EXP.-.....**” en concepto de garantía.....(4), para responder de las obligaciones, penalidades y demás gastos que se puedan derivar conforme a las normas y demás condiciones administrativas precitadas frente al asegurado.

El asegurador declara, bajo su responsabilidad, que cumple los requisitos exigidos en el artículo 57.1 del Reglamento General de la Ley de Contratos de las Administraciones Públicas.

La falta de pago de la prima, sea única, primera o siguientes, no dará derecho al asegurador a resolver el contrato, ni éste quedará extinguido, ni la cobertura del asegurador suspendida ni éste liberado de su obligación, caso de que el asegurador deba hacer efectiva la garantía.

El asegurador no podrá oponer al asegurado las excepciones que puedan corresponderle contra el tomador del seguro.

El asegurador asume el compromiso de indemnizar al asegurado al primer requerimiento de la INSTITUCIÓN FERIAL DE MADRID (IFEMA).

El presente seguro de caución estará en vigor hasta que la INSTITUCIÓN FERIAL DE MADRID (IFEMA) autorice su cancelación o devolución.

Lugar y fecha

Firma:

Asegurador.

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

Instrucciones para la cumplimentación del modelo.

- (1) Se expresará la razón social completa de la entidad aseguradora.
- (2) Nombre y apellidos del apoderado o apoderados.
- (3) Nombre de la persona asegurada.
- (4) Indicar modalidad del seguro de que se trata en función de que será garantía provisional o definitiva

ANEXO VII

(Este anexo relleno por el licitador se deberá incluir en el Sobre o archivo electrónico nº 1)

MODELO DE DECLARACIÓN RESPONSABLE DE SOMETIMIENTO A LA JURISDICCIÓN ESPAÑOLA

D.....
con D.N.I. o documento que lo sustituya nº, actuando en su nombre (o en representación de la empresa), frente a IFEMA y con relación al expediente para la contratación de.....
.....

DECLARA BAJO SU RESPONSABILIDAD

Que para todas las incidencias que de modo directo o indirecto pudieran surgir en relación con el cumplimiento, efectos o extinción del Contrato, la empresa licitadora que suscribe se somete a la **jurisdicción de los Juzgados y Tribunales españoles de cualquier orden**, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponderles.

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

ANEXO VIII

(Se deberá aportar en el momento que se requiera al licitador que ha presentado la mejor oferta según la cláusula 19 del Pliego de Cláusulas Administrativas Particulares)

MODELO DE DECLARACIÓN RESPONSABLE REGISTRO LICITADORES

Frente a IFEMA y dentro del procedimiento de licitación del contrato, D.
....., con D.N.I. núm.
....., mayor de edad, en nombre propio (o en representación de la empresa
....., con C.I.F. núm.
....., y domicilio en, calle
....., núm.),

DECLARA BAJO SU RESPONSABILIDAD:

1.- Que los datos anotados en el registro de licitadores presentado en esta licitación están vigentes y no han sufrido modificación alguna.

(En caso afirmativo se deberán indicar las variaciones o modificaciones que hayan tenido lugar así como aportar los documentos que lo acrediten).

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

ANEXO IX

(Este anexo relleno por el licitador se deberá incluir en el Sobre o archivo electrónico nº 3)

MODELO DE OFERTA ECONÓMICA

D., con D.N.I. núm., mayor de edad, en nombre propio (o en representación de la empresa, con C.I.F. núm., y domicilio en, calle, núm., una vez enterado de las condiciones exigidas para optar a la adjudicación del “..... EXP.”, se compromete a realizarlo con sujeción al Pliego de Bases y sus Anexos, por la cantidad total deEuros,..... Euros (en letras y cifras) (IVA EXCLUIDO). Esta cifra supone una baja del por ciento, respecto al presupuesto base de licitación.

....., de de 2020

Fdo.:

(Firma y sello de la empresa)

FICHA CRITERIOS OBJETIVOS DE VALORACIÓN (Sobre 3)

Se debe marcar con una "X" la opción ofertada:

CRITERIO D.- MEJORA INDICADORES DE NIVEL DE SERVICIO

D.1) INDICADORES DE GESTIÓN DE LA CALIDAD

Cálculo de la puntuación:

- Indicador CAL04 "NO CONFORMIDAD"

≤1 _____
2 _____
≥ 3 _____

D.2) INDICADORES DE GESTIÓN DE LA CALIDAD

Cálculo de la puntuación:

- Indicador CAL05 "CUMPLIMIENTO DE LA PLANIFICACIÓN"

0 _____
1 _____
≥ 2 _____

CRITERIO E.- JORNADAS ADICIONALES PARA PROYECTO

Jornadas de perfil de técnico senior adicionales sin coste para IFEMA, además de las 80 jornadas por dos años. Cálculo de la puntuación:

20 Jornadas más de técnico Senior _____
10 Jornadas más de técnico Senior _____
0 Jornadas más de técnico Senior _____

..... de de 2020

Firma del representante legal

FICHA –A- Sobre 3

PONDERACIÓN CRITERIO F

Descripción	Presupuesto máximo de licitación (euros)	Licencias		SOC	Total (euros) (I)
		CheckPoint	Ironport		
Parte Fija	210.004 €				

Descripción	Presupuesto máximo de licitación (euros)	Número de Jornadas	Precio unitario (euros) por Técnico/Jornada	Total (euros) (II) 80x Precio por Jornada
Parte Variable	35.000 €	80		

La suma del Total I+ Total II debe ser igual al importe de la oferta económica.

....., de de 2020

Firma del representante legal

ANEXO X

MODELO DE DECLARACIÓN DE CONFIDENCIALIDAD

(Su presentación es opcional, de conformidad con lo dispuesto en la cláusula 39 del Pliego, y sólo en caso de que se presente, se podrá incluir en el sobre o archivo electrónico en cuyo contenido se incluyan los datos o informaciones sobre los que solicita la reserva o confidencialidad).

D.....

con D.N.I. o documento que lo sustituya nº, actuando en su nombre (o en representación de la empresa), frente a IFEMA y con relación al expediente para la contratación de.....
.....

DECLARA BAJO SU RESPONSABILIDAD

1.- Que los siguientes datos o informaciones contenidas en su proposición son especialmente sensibles y tienen el carácter de confidenciales:

(Se identificarán de manera precisa y detallada, a qué datos debe extenderse ese derecho de confidencialidad y una breve justificación al respecto.)

2.- Que presta su consentimiento a que dichos datos o informaciones sean tratados exclusivamente por el órgano de contratación (y Comisión de Compras y Contratación) a los efectos de admisión y valoración de ofertas,

A los efectos,

Solicita que dichos datos e informaciones, sólo sean tratados por el órgano de contratación y Comisión de Compras y Contratación) con el carácter se reservados y confidenciales, siempre que con ello no se vulneren ni los principios de transparencia y publicidad, ni los derechos de protección jurídica efectiva y adecuada defensa de los intereses del resto de licitadores.

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

ANEXO XI

(Se deberá aportar en el momento que se requiera al licitador que ha presentado la mejor oferta según la cláusula 19 del Pliego de Cláusulas Administrativas Particulares)

SOLVENCIA ECONÓMICO-FINANCIERA

D.....
con D.N.I. o documento que lo sustituya nº, actuando en su nombre (o en representación de la empresa), frente a IFEMA y con relación al expediente para la contratación de.....
.....

DECLARA BAJO SU RESPONSABILIDAD

La compañía a la que represento tuvo una cifra de negocios global en los años 2016, 2017 y 2018 (IVA EXCLUIDO) de:

AÑO 2017:

AÑO 2018:

AÑO 2019:

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

ANEXO XII

(Se deberá aportar en el momento que se requiera al licitador que ha presentado la mejor oferta según la cláusula 19 del Pliego de Cláusulas Administrativas Particulares)

SOLVENCIA TÉCNICA

D.....
con D.N.I. o documento que lo sustituya nº, actuando en su nombre (o en representación de la empresa), frente a IFEMA y con relación al expediente para la contratación de.....
.....

DECLARA BAJO SU RESPONSABILIDAD

Se cumplimentará según proceda.

1.- Que la empresa que representa ha realizado los contratos de servicio dedurante los 3 últimos años (a contar desde), por importe superior a euros, que se adjuntan a continuación:

Referencia 1

Descripción del servicio:
Fechas de realización:
Destinatario:
Importe:

Referencia 2

Descripción del servicio:
Fechas de realización:
Destinatario:
Importe:

Referencia 3

Descripción del servicio:
Fechas de realización:
Destinatario:
Importe:

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)



IFEMA

**Feria de
Madrid**

**DOCUMENTACIÓN DE LA DIRECCIÓN DE
TECNOLOGÍAS DE LA INFORMACIÓN**

Departamento de Sistemas

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

AUTOR: Área de Sistemas de la Información y Ciberseguridad
FECHA DE CREACIÓN: 13 de Septiembre de 2019
Última versión: 22 de abril de 2020

ÍNDICE

A. CONDICIONES GENERALES DE DISEÑO, IMPLANTACIÓN, EXPLOTACIÓN Y ACCESO A LOS SISTEMAS DE IFEMA.....	17
<i>Seguridad.....</i>	<i>17</i>
<i>Dimensionamiento.....</i>	<i>17</i>
<i>Pruebas de carga.....</i>	<i>17</i>
<i>Alta disponibilidad y redundancia.....</i>	<i>17</i>
<i>Conformidad con normativa de Protección de Datos.....</i>	<i>17</i>
<i>Infraestructura virtual.....</i>	<i>18</i>
<i>Inicios, apagados y reinicios consistentes automáticos.....</i>	<i>18</i>
<i>Actualizaciones.....</i>	<i>18</i>
<i>Monitorización.....</i>	<i>18</i>
<i>Copia de seguridad.....</i>	<i>18</i>
<i>Logs.....</i>	<i>18</i>
<i>Operaciones periódicas de mantenimiento de sistemas automáticas.....</i>	<i>18</i>
<i>Manual de operaciones de sistemas.....</i>	<i>19</i>
<i>Condiciones de Soporte.....</i>	<i>19</i>
<i>Autenticación y Autorizaciones de los usuarios.....</i>	<i>19</i>
<i>Confidencialidad de los datos.....</i>	<i>20</i>
<i>Devolución de servicio.....</i>	<i>20</i>
<i>Integraciones con otros productos o servicios.....</i>	<i>20</i>
<i>Tratamientos con datos sensibles.....</i>	<i>20</i>
B. ACCESO A LA INFORMACIÓN.....	22
C. SEGURIDAD EN LAS COMUNICACIONES Y RECURSOS DE RED.....	25
D. SEGURIDAD EN LAS ESTACIONES DE TRABAJO.....	27

1. Condiciones generales de diseño, implantación, explotación y acceso a los sistemas de IFEMA

Cualquier producto o servicio relacionado con los recursos informáticos de IFEMA, 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 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 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 pueda adoptar los compromisos y las decisiones informadas más adecuadas en materia de sistemas para IFEMA.

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

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.

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 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 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.

Los datos, tratamientos, diseños y toda la información que pertenece a IFEMA 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.

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 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 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, 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 y con sus versiones más modernas, según se vaya actualizando. Se documentarán y comprobarán, de acuerdo con IFEMA, 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 para IFEMA 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 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 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, se podrían pactar condiciones de soporte diferentes. Por ejemplo: para soluciones no críticas el soporte podría ser 14x7x365, en horario laboral de IFEMA, 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. 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.

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 fuercen 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 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. El proveedor deberá devolver todo lo necesario a IFEMA para poder continuar con el servicio en otro proveedor "Cloud" u "On Premise", en el formato y forma que IFEMA 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

2. B. Acceso a la Información

En el caso en que la solución conste de acceso a la información o a los tratamientos de IFEMA, 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 y su Política de Seguridad. IFEMA entregará al adjudicatario el documento de normativa interna, perteneciente a la Política de Seguridad de IFEMA, 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, 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 y sólo desde aquellos puestos (terminales) y emplazamientos debidamente autorizados, y sólo a los recursos, tratamientos e información autorizados por IFEMA.
- El adjudicatario informará de cualquier cambio de su personal con autorización de acceso a los tratamientos o sistemas informáticos de IFEMA con tiempo suficiente para la revocación/autorización de sus accesos. Se deberá proporcionar por parte del adjudicatario una lista de usuarios autorizados por IFEMA para acceder a la plataforma, además de auditar y controlar quien accede, en que momento y con qué objetivo
- IFEMA 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 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 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 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. Cualquier ampliación del horario del servicio sólo podrá ser autorizado por IFEMA 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 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 deberá firmar el correspondiente Acuerdo de Confidencialidad y recibirá unas las Normas de Uso de Sistemas de IFEMA.

- 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. No está permitido acceder a los recursos de IFEMA no autorizados expresamente por IFEMA. Se accederá únicamente a los recursos, datos, servicios y aplicaciones autorizadas.
- El uso de los recursos informáticos de IFEMA se ajustará a lo estipulado en las presentes condiciones y únicamente con el propósito de acometer exclusivamente los fines y objetivos de IFEMA.
- No deberán imprimirse en papel, grabarse ni obtener copias de los datos procedentes de IFEMA 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.
- Ningún usuario deberá poseer, para usos no propios de su responsabilidad u objeto del contrato, material o información alguna propiedad de IFEMA, tanto ahora como en el futuro..
- Todos los recursos informáticos disponibles, son propiedad de IFEMA 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.
- 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, 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, 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 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 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, 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 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 cualquier responsabilidad al respecto.
- IFEMA 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, 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, dicha interconexión no deberá plantear ningún riesgo para IFEMA, 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; se compromete además a cumplir los estándares de comunicación en que se basa la arquitectura de red de IFEMA, por ejemplo adaptándose a la configuración de los elementos de seguridad tales como firewalls, proxys, etc. de IFEMA.
- 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 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
- 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 o propuestas alternativas que garanticen las comunicaciones entre las instalaciones del proveedor y las de IFEMA, 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.
- 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 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.
- Estos requerimientos técnicos pueden ser modificados por IFEMA por necesidades de negocio o técnicas y ningún cambio puede ser abordado por el adjudicatario sin consentimiento de IFEMA.

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, es necesario que dichas estaciones no planteen ningún riesgo para IFEMA, 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 y garantice el funcionamiento del servicio y el cumplimiento de los acuerdos sobre el mismo consensuados con IFEMA. El adjudicatario deberá soportar la posible instalación de aplicaciones cliente-servidor, que pudieran ser utilizadas en función de cómo decida implementar IFEMA el acceso por los operadores.
- En todo momento el adjudicatario deberá seguir las instrucciones que IFEMA 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 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 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.
- 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 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 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.

ANEXO XIV

CONSENTIMIENTO EXPRESO CONCEDIDO A IFEMA PARA LA SOLICITUD DE INFORMACIÓN

D.....
con D.N.I. o documento que lo sustituya nº, actuando en su nombre (o en representación de la empresa), frente a IFEMA y con relación al expediente para la contratación de.....
.....

CONSIENTE EXPRESAMENTE Y AUTORIZA

Que IFEMA pueda solicitar información, relacionada con el cumplimiento de las obligaciones de la empresa a la que represento en el marco del contrato adjudicado, ante la Seguridad Social, Agencia Tributaria u otros organismos o instancias administrativas o judiciales.

En....., a.....de.....de 2020

Fdo.:.....
(Firma y sello de la empresa)

ANEXO XV

MODELO DE DOCUMENTO DE FORMALIZACIÓN DEL CONTRATO

En Madrid, a

REUNIDOS

De una parte, **D.**, con D.N.I. núm.

Y de otra, **D.**, mayor de edad, con D.N.I. núm:.....

INTERVIENEN

D., como Director General de la Institución Ferial de Madrid, en adelante **IFEMA**, con C.I.F. nº Q-28/73018-B, con domicilio social en Avenida del Partenón, 5 (28042) Madrid;

D., en representación de,, en adelante el "**Adjudicatario**", con N.I.F., y domicilio social en (.....) de

MANIFIESTAN

1. Que en el procedimiento seguido por IFEMA para la adjudicación del contrato de servicios denominada "- *Expediente*", solicitó ofertas con arreglo al Pliego de Cláusulas Administrativas Particulares del referido Expediente, que forma parte integrante del presente contrato y que ha sido aceptado incondicionalmente por el Adjudicatario mediante la presentación de su oferta.
2. Que IFEMA, como resultado del referido procedimiento, ha adjudicado el contrato a la oferta presentada por el Adjudicatario, quien ha manifestado que cumple con todos los requisitos para contratar con IFEMA.
3. Que en virtud de lo dispuesto en la Cláusula 24 del referido Pliego de Cláusulas Administrativas Particulares, las partes proceden a la formalización del presente contrato, del cual formarán parte, y con el mismo carácter contractual, la oferta adjudicataria y el citado Pliego con el resto de documentación señalada en el mismo.

Por tanto, ambas partes se reconocen capacidad legal para celebrar el presente contrato, de acuerdo con las siguientes

CLÁUSULAS

1. - OBJETO DEL CONTRATO

Constituye el objeto del presente contrato la ejecución por el Adjudicatario de los servicios de de acuerdo con lo recogido en el Pliego de Prescripciones Técnicas, la oferta presentada por el Adjudicatario y el Pliego de Cláusulas Administrativas Particulares del Expediente de referencia con el resto de documentación que en el mismo y en sus Anexos se señalen, que forman parte integrante del presente contrato.

2. - PRECIO DEL CONTRATO.-

IFEMA como contraprestación por los servicios prestados, abonará al Adjudicatario el siguiente precio señalado en su oferta:

[] Precios unitarios: De acuerdo con los precios cerrados unitarios recogidos en la oferta presentada por el Adjudicatario y lo dispuesto en el Pliego de Cláusulas Administrativas Particulares para la determinación del precio del contrato, el importe total queda determinado en (.....€) más el IVA correspondiente.

[] A tanto alzado: De acuerdo la oferta presentada por el Adjudicatario y lo dispuesto en el Pliego de Cláusulas Administrativas Particulares para la determinación del precio del contrato, el precio total alzado y cerrado del contrato queda determinado en (.....€) más el IVA correspondiente.

[] Otra modalidad: De acuerdo la oferta presentada por el Adjudicatario y lo dispuesto en el Pliego de Cláusulas Administrativas Particulares para la determinación del precio del contrato.....

3.- PLAZO DE EJECUCIÓN.-

El Adjudicatario iniciará los trabajos objeto del presente contrato al día siguiente de su fecha de formalización y tendrá una duración de

Y en prueba de conformidad de cuanto antecede, firman ambas partes, en las representaciones que respectivamente ostentan, el presente documento por duplicado, en la fecha y lugar indicados en el encabezamiento.

Por IFEMA

Por

Fdo.:

(Órgano de contratación)

Fdo.:

(Representante Legal)

ANEXO XVI COMPROMISO DE CONFIDENCIALIDAD

A las empresas que lo solicite se les facilitará, previa rúbrica del correspondiente **compromiso de confidencialidad cumplimentado, junto con una copia de la escritura de poder.**

COMPROMISO DE CONFIDENCIALIDAD

“SERVICIO DE SOPORTE PARA CIBERSEGURIDAD DE LA INSTITUCIÓN FERIAL DE MADRID”

EXP.- 20/173- 2000017805”

D., con D.N.I. núm., en representación de la entidad (en adelante la “Compañía”) en su calidad de ; con C.I.F. núm y domicilio social en,; de acuerdo con las facultades conferidas por escritura otorgada ante el Notario de D., de fecha de de, con el número de orden de su protocolo.

Durante el proceso de oferta y licitación IFEMA pondrá a disposición de la Compañía, determinada información relativa al Proyecto para la Contratación del “SERVICIO DE ADMINISTRACIÓN Y GESTIÓN DE SISTEMAS Y APLICACIONES WEB DE IFEMA, EL ALOJAMIENTO DE ESTAS Y SUS ESTRUCTURAS EN LA NUBE” (en adelante el “Proyecto”) para habilitar la remisión y presentación por parte de la Compañía de su oferta (en adelante, la “Oferta”), siempre y cuando los términos y condiciones establecidos en el presente Compromiso de Confidencialidad (el “Compromiso”) sean aceptados por la Compañía.

A los efectos del presente documento, se entiende por “Información Confidencial”, toda la información financiera, comercial, técnica, operativa, de personal, de gestión, base de datos, datos personales, know how o cualquier otra información, relativa a IFEMA y/o el Proyecto, que pueda ser suministrada ya sea por escrito, oralmente o de cualquier otra forma por IFEMA y/o sus agentes, asesores profesionales, empleados o administradores, así como todos los análisis, compilaciones, estudios u otros documentos preparados por la Compañía o por cualquiera de sus Representantes y que contengan o, de una forma u otra, reflejen o se basen en tal información.

Por la presente manifiesta su compromiso formal de guardar la más rigurosa reserva y confidencialidad en relación con la Información Confidencial que en este acto se le entrega o que la Compañía obtenga con posterioridad durante el citado proceso de licitación, así como de cuanta información obtenga, cualquiera que sea su soporte y forma de comunicación, en las visitas programadas a las instalaciones o la que pudiera obtener por cualquier otro conducto con posterioridad a esta fecha y, en general cualquier información que por su naturaleza y/o las circunstancias en que se produzca la revelación, deba de buena fe estimarse

como confidencial.

La citada información confidencial será tratada como tal por el receptor y no será revelada sin el consentimiento previo de IFEMA. En particular, el receptor se compromete a adoptar las medidas de seguridad técnicas y administrativas necesarias para evitar que terceros no autorizados puedan acceder a la Información Confidencial, el procesamiento ilegal o la pérdida, distribución o daño accidental de la misma y a limitar su acceso a los empleados autorizados que precisen disponer de ella para la formulación de la Oferta, trasladándoles idéntica obligación de confidencialidad.

En el supuesto de que la Compañía tenga acceso a datos de carácter personal durante la fase de licitación y que resulten necesarios para la correcta preparación de la Oferta, la Compañía se obliga expresamente a observar todos los requerimientos impuestos por las leyes de protección de datos o de protección de la privacidad vigentes que resulten aplicables.

La Compañía se obliga a utilizar la Información Confidencial suministrada única y exclusivamente con la finalidad de evaluar el Proyecto y preparar la Oferta a presentar a los efectos de la licitación promovida por IFEMA.

Una vez adjudicado el Proyecto, o en el momento de conclusión del periodo de licitación si la Compañía no hubiese presentado Oferta, la Compañía destruirá o devolverá, según así le sea indicado por IFEMA y de forma inmediata la Información Confidencial y todas las copias de la misma sin posibilidad de retener copia alguna; asimismo, procederá a borrar la Información Confidencial de cualquier programa de ordenador o sistema informático al que la hubiera incorporado y a destruir los materiales preparados por la Compañía a partir de la Información Confidencial. La Compañía deberá acreditar la devolución o destrucción de toda la Información Confidencial mediante la emisión de un certificado a favor de IFEMA. No obstante lo anterior, en la medida en que la Compañía resulte adjudicataria del Proyecto, ésta podrá conservar aquella Información Confidencial que resulte necesaria para el posterior desarrollo del Proyecto, todo ello de conformidad con los términos aquí previstos y/o con los que deban regir la relación entre ambas partes a partir de la adjudicación.

La Compañía se obliga a indemnizar y a mantener indemne a IFEMA, así como a sus accionistas, consejeros y directivos por cualesquiera daños, pérdidas, sanciones, costos y gastos que se deriven del uso no autorizado o la revelación indebida de la Información Confidencial y en general de la infracción de los compromisos y obligaciones de confidencialidad aquí contenidos, de cualquier otro incumplimiento de las disposiciones de presente Compromiso o de cualesquiera leyes sobre protección de datos o protección de la privacidad que resulten aplicables.

ANEXO XVII NORMAS PARA EL ACCESO A LOS RECURSOS DE IFEMA Y MEDIDAS DE
SEGURIDAD



DOCUMENTACIÓN DE LA DIRECCIÓN DE
TECNOLOGÍAS DE LA INFORMACIÓN

Departamento de Sistemas

**Política de Seguridad de
Feria de Madrid: Normas del Personal
Externo con acceso a los Recursos
Informáticos de Ifema**

AUTOR: Feria de Madrid
FECHA DE CREACION: 28 de Enero de 2008
ÚLTIMA VERSIÓN: 5 de noviembre de 2018

ÍNDICE

A. OBJETIVO	35
<i>Reservados todos los derechos ©.....</i>	35
B. APLICACIÓN DE ESTAS NORMAS DEL PERSONAL	35
B.1. Definiciones	35
B.2. Ámbito de aplicación	36
<i>Ámbito personal</i>	36
<i>Ámbito material</i>	36
C. FUNCIONES Y OBLIGACIONES DEL PERSONAL.....	36
<i>Identificadores de usuario, claves de acceso y dispositivos de autenticación de dos factores</i>	36
<i>Salvaguarda de los recursos informáticos de Feria de Madrid.....</i>	37
<i>Confidencialidad de la información.....</i>	38
<i>Normas de etiqueta</i>	39
<i>Incidencias</i>	39
<i>Puestos de trabajo</i>	40
D. CONTACTAR CON LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y EL DELEGADO DE PROTECCIÓN DE DATOS	40

- **Objetivo**

Estas normas del Personal se han elaborado de conformidad con 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, según los cuales el personal externo de Feria de Madrid que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio de Feria de Madrid. Estas normas forman parte de la Política de Seguridad de Feria de Madrid.

Estas Normas del Personal son un documento de mínimos; las medidas de seguridad establecidas en este documento prevalecerán sobre cualquier otra política o plan de seguridad en caso de contradicción, sin perjuicio de normativas específicas vigentes más estrictas que existan para la administración y manipulación de los recursos informáticos protegidos.

Reservados todos los derechos ©

La Política de Seguridad de Feria de Madrid y sus Anexos son propiedad de Feria de Madrid. Está prohibida la reproducción, plagio, distribución, transmisión telemática o comunicación pública en todo o en parte de esta Política de Seguridad o sus Anexos sea cual fuere el medio o soporte empleados, sin la autorización expresa de Feria de Madrid.

3. aplicación de estas Normas del Personal

Definiciones

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso.

Sistema informático: Conjunto de ficheros, archivos, programas, soportes (discos, cintas, CD-ROM's...) y equipos (ordenadores, terminales, dispositivos de comunicaciones, red...) empleados para el almacenamiento y tratamiento de datos.

Recurso informático: Cualquier parte componente de un sistema informático.

Ámbito de aplicación

Ámbito personal

Estas Normas del Personal son de obligado cumplimiento para todo el personal que tenga acceso a los recursos informáticos de Feria de Madrid:

1. Personal contratado directamente por Feria de Madrid.
2. Personal contratado por empresas de trabajo temporal para prestar sus servicios en Feria de Madrid.
3. Personal de empresas de servicios contratadas por Feria de Madrid.
4. Personal de empresas colaboradoras con Feria de Madrid.

Todas las personas relacionadas anteriormente se encuentran obligadas por ley a cumplir lo establecido en este documento y están sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Ámbito material

Todos los recursos informáticos de Feria de Madrid.

4. Funciones y obligaciones del personal

Con el objeto de dar debido cumplimiento a la normativa en materia de protección de datos personales, resultan de aplicación 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. Feria de Madrid impone a todo el personal con acceso a sus recursos informáticos las siguientes obligaciones, las cuales deberán ser conocidas, aceptadas y respetadas por todos. Obligaciones de todo el personal con acceso autorizado a los recursos informáticos

Feria de Madrid pone sus recursos informáticos a disposición de los usuarios autorizados, a quienes se confía y encomienda su explotación para realizar tareas relacionadas con la actividad de Feria de Madrid y dentro de los cometidos y funciones del puesto de trabajo desempeñado por cada usuario.

El usuario autorizado para acceder a los recursos informáticos de Feria de Madrid es responsable de aprovechar y preservar los recursos puestos a su disposición, sin desviarlos de sus objetivos sustanciales.

Identificadores de usuario, claves de acceso y dispositivos de autenticación de dos factores

1. No se puede comunicar a otra persona, física o jurídica, el identificador de usuario ni la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento Feria de Madrid, con el fin de que le asigne una nueva clave.
2. Las operaciones susceptibles de seguimiento que se realicen en la red corporativa o intranet de Feria de Madrid quedarán registradas en los archivos LOG de los servidores. El uso del identificador y la clave asignados a cada usuario implicará la aceptación, como documento probatorio de la operación efectuada, de los registros generados en dichos archivos LOG y almacenados en el sistema informático de Feria de Madrid. Salvo prueba en contrario, se presumirá 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.
3. Si el usuario debe escoger su propia clave de acceso, aplicará las siguientes medidas, conducentes a garantizar su seguridad y a impedir que pueda desvelarse de forma fortuita o intencionada:

- La clave de acceso constará como mínimo de ocho caracteres, entre cifras y letras.
 - No se emplearán en la clave de acceso combinaciones triviales tales como su identificador de usuario, su nombre propio, su apellido, su teléfono, la matrícula de su coche...
 - Se debe utilizar palabras inventadas.
 - La clave de acceso no debe reutilizarse. Cuando se requiera que el usuario cambie su clave de acceso, deberá proporcionar una clave nueva y no podrá suministrar la empleada con anterioridad.
 - Es aconsejable que el usuario memorice su clave de acceso. En ningún caso deberá dejarse escrita en lugares accesibles. Durante su vigencia dichas claves de acceso se almacenarán de un modo ininteligible.
 - Las claves de accesos habrán de ser modificadas con una periodicidad en ningún caso superior a un año.
4. Los usuarios que reciban dispositivos de autenticación de dos factores, como los tokens SafeWord, para acceder a las aplicaciones de Feria de Madrid, tomarán todas las medidas necesarias para custodiarlos con eficacia.
 5. Se deberá notificar inmediatamente a Feria de Madrid todos los casos en que personas no autorizadas pudieran tener acceso a los dispositivos de autenticación.
 6. Asimismo, deberán notificarse inmediatamente todos los casos de extravío o sustracción de los dispositivos de autenticación.
 7. El usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificador de usuario o su dispositivo de autenticación de dos factores.

Salvaguarda de los recursos informáticos de Feria de Madrid

Para preservar con eficacia los recursos informáticos de Feria de Madrid, el usuario con acceso autorizado a los mismos debe conocer y observar las normas generales siguientes, sin perjuicio de otras normativas específicas más estrictas que pudieran estar en vigor:

1. Los usuarios acceden a los ficheros de Feria de Madrid por medio de las opciones de las aplicaciones relacionadas con sus funciones y puesto de trabajo, cuyo uso tengan autorizado, limitado por el perfil asignado por el administrador de sistemas.
2. El usuario se abstendrá de intentar distorsionar o falsear los registros LOG del sistema.
3. Tampoco intentará descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Feria de Madrid.
4. No se deben destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de Feria de Madrid o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
5. Debe evitarse obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de Feria de Madrid, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
6. No está permitido intentar acceder a áreas restringidas de los sistemas informáticos de Feria de Madrid o de terceros.

7. El nivel de privilegios de un usuario en el sistema siempre será el adecuado para las funciones y objetivos asociados a su puesto de trabajo. El usuario no intentará aumentarlo.
8. Voluntariamente nunca se introducirán programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de Feria de Madrid o de terceros. El usuario tendrá la precaución de utilizar los programas anti-virus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
9. Los recursos informáticos y telemáticos de Feria de Madrid, no se desviarán hacia actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

Confidencialidad de la información

1. No está permitido enviar datos de carácter personal o información confidencial de Feria de Madrid a terceros, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.
2. Los usuarios de los sistemas de información corporativos 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 Feria de Madrid, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato o de la relación laboral.
3. Ningún usuario deberá poseer, para usos no propios de su responsabilidad, material o información alguna propiedad de Feria de Madrid, tanto ahora como en el futuro.
4. El usuario no deberá grabar ni obtener copias de los datos de carácter personal procedentes de los ficheros de Feria de Madrid en ningún dispositivo de almacenamiento (disquetes, CD-ROM grabables, cintas...) incluyendo los discos duros de los equipos empleados para el acceso remoto.
5. Todos los datos disponibles a través del acceso remoto son propiedad de Feria de 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 Feria de Madrid.
6. El usuario deberá emplear un programa antivirus en los equipos utilizados para acceder remotamente a la red corporativa de Feria de Madrid.
7. El usuario se compromete a respetar las instrucciones específicas en materia de seguridad que pudiera recibir desde Feria de Madrid.
8. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, 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 Feria de 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 Feria de Madrid, no supondrá, en ningún caso, una modificación de esta cláusula.

9. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y dará derecho a Feria de Madrid a exigir una indemnización económica.

Normas de etiqueta

1. No está permitido introducir contenidos obscenos, inmorales u ofensivos en la red corporativa de Feria de Madrid.
2. No está permitido enviar contenidos obscenos, inmorales u ofensivos desde la red corporativa o los puestos de trabajo de Feria de Madrid.
3. El empleo de los recursos informáticos debe ser siempre acorde con el prestigio y la imagen corporativa de Feria de Madrid, especialmente si se proyecta al exterior.

Incidencias

Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad.

Serán de aplicación las normas legales en materia de protección de datos personales como 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, con el fin de:

- Permitir la resolución de las incidencias en el menor plazo posible.
- Anotar las incidencias en el Registro de Incidencias.
- Garantizar la seguridad de los ficheros de Feria de Madrid.
- Prevenir los posibles ataques a la seguridad de los ficheros de Feria de Madrid.
- Perseguir las responsabilidades que pudieran derivarse de las incidencias.

Feria de Madrid establece las medidas contenidas en este apartado:

1. Es obligación de todo el personal con acceso a los recursos informáticos de Feria de Madrid comunicar al Delegado de Protección de Datos (DPD) y a la Dirección de Tecnologías de la Información, inmediatamente, cualquier incidencia que detecte y que afecte o pueda afectar a la seguridad de los datos.
2. Dicha comunicación deberá realizarse inmediatamente, y, en cualquier caso, en un plazo de tiempo no superior a una hora desde el momento en que se conozca dicha incidencia. La comunicación se realizará a través de cualquiera de estos medios, por orden de prioridad:
 - Teléfono de la Dirección de Tecnologías de la Información: 91 722 50 45
 - Correo electrónico de la Dirección de Tecnologías de la Información: dinformatica@ifema.es
 - Correo electrónico del Delegado de Protección de Datos (DPD): dpd@ifema.es
3. Quien conociera de una incidencia y no la comunicara siguiendo estas normas, incurrirá en una falta contra la seguridad del sistema de información. Ante los graves perjuicios que se pueden ocasionar, Feria de Madrid actuará disciplinariamente en el supuesto de no actuar con la máxima diligencia ante una irregularidad en el funcionamiento habitual del sistema informático.

Puestos de trabajo

1. Los puestos de trabajo estarán bajo la responsabilidad de los usuarios autorizados que los utilizan.
2. Los usuarios garantizarán que la información que muestran sus puestos de trabajo no pueda ser vista por personas no autorizadas.
3. 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 datos protegidos.
4. Cada ordenador dispondrá de un protector de pantalla con contraseña que se activará a los diez minutos de inactividad y no estará permitido desactivarlo.
5. En el caso de las impresoras, el usuario deberá asegurarse de que no quedan 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.

5. Contactar con la Dirección de Tecnologías de la Información y el delegado de protección de datos

Teléfono de la Dirección de Tecnologías de la Información: 91 722 50 45

Correo electrónico de la Dirección de Tecnologías de la Información: dinformatica@ifema.es

Correo electrónico del Delegado de Protección de Datos: dpd@ifema.es