C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

PLAN DE MEDIDAS PARA LA PREVENCIÓN DEL FRAUDE, EL CONFLICTO DE INTERESES Y LA CIBERSEGURIDAD

FUNDACIÓ COMUNITAT VALENCIANA-REGIÓ EUROPEA

NOVIEMBRE DE 2022

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

1. PREÁMBULO

La Convención de Naciones Unidas contra la Corrupción (Nueva York, 31/10/2003) es un instrumento internacional que forma parte de nuestro ordenamiento jurídico al haber sido ratificada por el Estado español y publicada en el BOE, núm. 171, de 19 de junio de 2006. Este documento puso de manifiesto que la corrupción había dejado de ser un problema local para convertirse en un fenómeno transnacional que afecta a todas las sociedades y economías, lo que hace esencial la cooperación internacional para prevenirla y luchar contra ella. De igual modo señalaba que la corrupción es un fenómeno generador de problemas y amenazas para la estabilidad y seguridad de las sociedades al socavar las instituciones y los valores de la democracia, la ética y la justicia y al comprometer el desarrollo sostenible y el imperio de la ley.

Según datos de Transparencia Internacional, en su Informe sobre el índice de Percepción de la Corrupción (IPC) publicado el 28 de enero de 2021, España se sitúa en el puesto 32. Este Informe pone de manifiesto la influencia de la corrupción en la acción de los gobiernos frente a la pandemia SARS-2/COVID-19, comparando la puntuación de cada país en el índice con su inversión en salud y con la medida en que las normas e instituciones democráticas se han debilitado durante la pandemia. Todo ello conlleva la necesidad de que los Estados adopten medidas e instrumentos encaminados a prevenir y combatir el fraude, la corrupción, pero también a promover la integridad, la obligación de rendir cuentas y la debida gestión de los asuntos y los bienes públicos.

La OCDE define la integridad pública como "*La alineación consistente con, y el cumplimiento de, los valores, principios y normas éticos compartidos, para mantener y dar prioridad a los intereses públicos, por encima de los intereses privados, en el sector público*". Así, en su Manual sobre Integridad Pública (julio, 2020), aboga por formular una estrategia de integridad pública para apoyar un sistema de integridad coherente que, desde una perspectiva del sistema en su conjunto, y en base a informaciones y evidencias fruto de una reflexión profunda, adopte medidas encaminadas a la identificación, prevención y corrección de los principales riesgos para la integridad pública.

De igual modo, el IV Plan de Gobierno Abierto (2020-2024) del Ministerio de Política Territorial y Función Pública, entre cuyos principales ejes figura el de integridad, está orientado a la construcción de un sistema de Integridad pública, fortaleciendo valores éticos y mecanismos para afianzar la integridad de las instituciones públicas y reforzar la confianza de la ciudadanía. Entre las iniciativas de la Comunitat Valenciana, se incluye la elaboración de una estrategia de integridad pública, siendo la Agencia Valenciana Antifraude (AVAF) considerada como actor público involucrado en el proceso.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

En el ámbito de la Comunitat Valenciana, el Cuaderno Pedagógico "*Radiografía de la corrupción pública. Jurisprudencia de los tribunales valencianos (1995-2018)*"[1], analiza las resoluciones judiciales en materia de corrupción pública dictadas por los tribunales valencianos durante este período, y ha servido de base para que el Observatori Ciutadà contra la Corrupció elabore el "Mapa de la Corrupción", permitiendo comprobar malas prácticas que han generado casos de corrupción de gran trascendencia y preocupación en el ámbito de nuestra Comunitat.

Por todos estos motivos, la Fundació Comunitat Valenciana-Regió Europea (en adelante FCVRE) ha elaborado el presente Plan de Medidas para la Prevención del Fraude, el Conflicto de Intereses y la Ciberseguridad, pues siendo una fundación perteneciente al sector público instrumental de la Generalitat Valenciana, financia sus actividades casi de forma exclusiva a través de fondos públicos que se reciben en forma de subvención nominativa. Existen numerosos motivos por los cuales es necesario para la FCVRE elaborar este Plan. Por un lado, los aspectos externos que lo aconsejan son:

- Aspectos normativos, que se desarrollarán en el siguiente punto.
- Aspectos técnicos, pues la necesidad de la elaboración del Plan ha sido indicada desde la propia Intervención General, quien cada ejercicio lleva a cabo la fiscalización de la actividad de la FCVRE, de sus procedimientos y de su gestión financiera.
- Aspectos sociales, ya que es un deber y una obligación del sector público y de las entidades que lo conforman ser transparentes ante la ciudadanía e instrumentar todos los mecanismos posibles para evitar las malas prácticas en el manejo de los fondos y en el desarrollo de sus actividades.
- Aspectos económicos, pues se tiene en cuenta que la utilización de fondos púbicos para el desarrollo de las actividades implica un uso racional y austero de los mismos, para lo cual es necesario activar todos los mecanismos necesarios para evitar desviaciones de fondos, eventuales fraudes, ataques que comprometan la tesorería de la entidad y evitar también posibles conflictos de intereses en el uso de estos fondos.

Por otro lado, existen una serie de aspectos de carácter interno que lo motivan y que están relacionados con la propia organización (cumplir con la legalidad vigente), con los profesionales que desarrollan su labor en ella (protegerlos antes amenazas externas), aspectos reputacionales (de cara a la ciudadanía y ante la propia administración

[1] CORRECHER MIRA, J. *Radiografía de la corrupción pública Jurisprudencia de los tribunales valencianos (1995-2018)*; Ed. Observatori Ciutadà contra la Corrupció, 2019.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

autonómica a la que la FCVRE pertenece) y también de planificación (incorporar las medidas recogidas en este plan a los procedimientos cotidianos).

Además, desde la AVAF se considera esencial que el Sector público instrumental de la Generalitat Valenciana cuente con un sistema de integridad pública, dadas sus especiales características organizativas y funcionales (a menudo la composición de su plantilla no es funcionarial, como es el caso de la FCVRE; en muchos casos, no se cuenta con la preceptiva figura del auditor interno, existe cierta relajación de requisitos en procedimientos de contratación o subvenciones, etc.). Es vital su integración y participación activa en el desarrollo y ejecución del plan de integridad pública.

2. MARCO NORMATIVO EN MATERIA DE TRANSPARENCIA, BUEN GOBIERNO Y CONFLICTO DE INTERESES

El ordenamiento jurídico español recoge una serie de normas a las cuales hay que atenerse en el ejercicio de sus funciones, tanto de miembros del gobierno y otros cargos de la administración, como de los que tienen la condición de empleados públicos o del personal laboral al servicio de la administración, como es el caso del personal de la FCVRE. Concretamente:

- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 53/2014, de 26 de diciembre, de incompatibilidades del personal al servicio de las Administraciones Públicas.

Además, es necesario recodar las obligaciones de publicidad contenidas en el Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y la Ley 38/2003, de 17 de noviembre, General de Subvenciones.

En el ámbito autonómico, la Ley 22/2018, de 6 de noviembre, de la Inspección General e Servicios y del Sistema de Alertas para la Prevención de las malas prácticas de la Administración de la Generalitat y su sector público instrumental, contempla un sistema preventivo de alertas dirigido a detectar irregularidades y malas prácticas administrativas en el ámbito de la gestión pública de la Administración de la Generalitat y su sector público instrumental. Esta ley crea también la Comisión Interdepartamental para la prevención de irregularidades y malas prácticas, con el desarrollo reglamentario mediante el Decreto 66/2019, de 26 de abril, del Consell.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

Por otra parte, la Ley 11/2016, de 28 de noviembre, de la Agencia de Prevención de la Lucha contra el Fraude, crea la Agencia de la Prevención y Lucha contra el Fraude y la Corrupción en la Comunitat Valenciana, con la finalidad de prevenir e investigar los posibles casos de uso o destinación irregular de fondos públicos y de conductas opuestas a la integridad o contrarias a los principios de objetividad, eficacia y sumisión plena a la ley y el derecho.

Así mismo, la Ley 1/2022, de 13 de abril, de Trasparencia y Buen Gobierno de la Comunitat Valenciana y el Decreto 56/2016, del Consell, de 6 de mayo, por la que se aprueba el Código de Buen Gobierno de la Generalitat Valenciana, establecen las normas de conducta que habrán de observar en sus actuaciones públicas los altos cargos de la Comunitat Valenciana, la obligación de transparencia en la actividad pública, la publicación de agendas institucionales y la política de obsequios y regalos.

También es necesario mencionar la Ley 25/2018, de 10 de diciembre, reguladora de la actividad de los grupos de interés de la Comunitat Valenciana y el Decreto 172/2021, de 15 de octubre, del Consell, que tienen por objetivo asegurar la transparencia en la participación de los grupos de interés en lo procesos de elaboración y aplicación de políticas públicas. Finalmente, es necesario destacar la Ley 4/2021, de 16 de abril, de la función pública valenciana, específicamente el capítulo IV que hace referencia a los deberes, el código ético y el régimen de incompatibilidades del personal funcionario al servicio de la Administración de la Generalitat.

3. OBJETO Y COMPETENCIAS DE LA ADMINISTRACIÓN PROMOTORA

El objeto del presente plan de medidas para la prevención del fraude, el conflicto de intereses y la ciberseguridad de la FCVRE es diseñar las principales acciones que ha de adoptarse en el seno de la entidad para evitar el mal uso o el fraude de sus recursos financieros, que provienen en su mayor parte de administraciones públicas en general y de la Generalitat Valenciana en particular. Son, por lo tanto, fondos públicos que es necesario gestionar con criterios de austeridad y eficiencia, sino también proteger con todas las medidas de seguridad disponibles para evitar su desvío o apropiación indebida.

La FCVRE es la entidad de la Generalitat Valenciana que se encarga de gestionar la oficina regional ubicada en Bruselas y por este motivo trabaja con proveedores de bienes y servicios tanto españoles como belgas. Además, su personal está ubicado en su gran mayoría en la delegación de Bruselas, donde además se encuentra el servidor a través del cual se gestiona y protege la documentación en versión digital con la que trabaja el personal. Esta parte de la plantilla se encarga de hacer el seguimiento de las políticas europeas que son de interés para la Comunitat Valenciana, su sector productivo y empresarial y su ciudadanía en general, así como la defensa de los intereses del gobierno valenciano en las instituciones comunitarias. Cuenta además con dos personas ubicadas en la Comunitat Valenciana; una en Alicante que gestiona el centro de información sobre

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

asuntos europeos Europe Direct Comunitat Valenciana-Alicante, abierto a toda la ciudadanía y financiado por la Comisión Europea; otra en Valencia con el puesto de técnico de gestión financiera y administrativa que se encarga de la gestión interna (económica, jurídica y del personal) de la FCVRE, así como de la relación con la administración autonómica.

La condición de entidad perteneciente al sector público instrumental y la gestión de fondo públicos hacen necesaria la implementación de medidas de protección tanto de carácter interno como hacia el exterior, de dichos fondos. Por otro lado, esta necesidad surge también por las recomendaciones provenientes tanto de la DGTIC (medidas de ciberseguridad) como de la propia Intervención General de la Generalitat Valenciana, quien aconsejó en la última auditoría de cuentas articular un sistema interno de control y protección ante el fraude y por posibles conflictos de intereses.

4. SUJETOS DESTINATARIOS DEL PLAN

Lo sujetos destinatarios del presente plan son todos los miembros de la plantilla de la FCVRE, pues, aunque solo una parte de ellos gestiona los recursos financieros, todos ellos manejan documentación sensible y de uso diario en el desempeño de sus funciones y competencias. Por ello, es necesario que todos tengan en cuenta las medidas en materia de ciberseguridad.

Por otro lado, la gestión financiera es una tarea compartida entre la persona que se encarga de la coordinación, la persona que ocupa el puesto de técnico de gestión administrativa y financiera y la persona que ocupa el puesto de administrativa en Bruselas. También interviene de manera decisiva la directora de la FCVRE, que es la Directora General de Relaciones con la UE y el Estado, quien no está contratada por la entidad, sino que depende directamente de Presidencia de la Generalitat y desarrolla su labor de gestión de la FCVRE por los poderes generales otorgados por el Patronato. Realiza estas funciones a título gratuito y en función de su cargo, pues así lo establecen los estatutos de la entidad. Todas estas personas que participan de una u otra manera en la gestión financiera se verán afectadas y deberán conocer las medias en materia de antifraude, ciberseguridad y conflicto de intereses que recojan este plan.

5. VIGENCIA Y DURACIÓN DEL PLAN Y EVALUACIÓN

El presente plan entrará en vigor a partir de su aprobación por el Patronato, previsiblemente el 1 de enero de 2023 y tendrá una duración indefinida.

La ejecución de sus medidas será evaluada anualmente para justarlas a las circunstancias que se vayan produciendo y a los resultados de dichas evaluaciones.

5. AUTOEVALUACIÓN INICIAL

Tomando como referencia la autoevaluación realizada por la presidencia de la Generalitat, se procede a analizar los siguientes aspectos relacionados con la prevención del fraude y los conflictos de interés. Las respuestas se corresponden con el momento previo a la elaboración, aprobación, difusión e implementación de las medidas contenidas

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

en este plan. Cada año se realizará una evaluación interna en que se volverán a plantear las mismas cuestiones con el fin de hacer seguimiento de cada una de las medidas.

En primer lugar, se analiza la situación actual en cuanto al conflicto de intereses y la lucha contra el fraude:

*Puntuación: 1 (no), 2 (parcial), 3 (habitual), 4 (sí)

PREGUNTAS GENERALES	Grado de cumplimiento				Justificación
	1	2	3	4	
¿Existe un plan de medidas para detectar y corregir el fraude, la corrupción y los conflictos de interés?	X				Está en proceso de elaboración, pero hasta ahora no se había abordado la necesidad en la entidad.
¿Existe un manual de procedimientos con suficientes garantías de seguridad en cuanto a la gestión de los fondos públicos?			X		Existe un manual que establece los procedimientos tanto de la actividad propia de Bruselas como de la gestión administrativa, financiera y del personal. Es auditado cada año.
¿Se realizan periódicamente auditorías de cuentas y de cumplimiento de la legalidad?				X	La Intervención General fiscaliza las cuentas anuales y la gestión operativa de la FCVRE, así como el cumplimiento de la legalidad vigente a través de una firma externa de auditoría cada ejercicio.
PREVENCIÓN					
¿Se dispone de una declaración institucional de compromiso de lucha contra el fraude, la corrupción y el conflicto de intereses?		X			La directora de la FCVRE, como órgano de contratación, firma una memoria en cada expediente de contratación en que declara que no existe conflicto de intereses en dicho proceso.
¿Se realiza una autoevaluación que identifique los riegos específicos, su impacto y la posibilidad de que ocurran, y se revisa periódicamente?		X			Desde hace dos años la auditoría operativa se centra en los riesgos de desvío de fondos a la hora de pagar a los proveedores y las posibles lagunas en los procesos de pago.
¿Se difunde un código ético y se informe sobre la política de obsequios?		X			La FCVRE no tiene elaborado un código ético. La directora publica los obsequios que recibe en el portal de transparencia de la GVA. La FCVRE tiene un enlace en su web a dicho portal.
¿Se imparte formación que facilite la detección del fraude y que promueva la ética pública?		X			La técnica financiera realiza la formación en materia impartida periódicamente por la DG de Sector Público y la DGTIC.
¿Se ha elaborado un procedimiento para tratar el conflicto de intereses?			X		Se ha introducido en los formularios relacionados con la contratación (memoria justificativa del gasto), pero no existe un procedimiento específico.
¿Rellenan una declaración de ausencia de conflicto de intereses todos los que intervienen en los procedimientos de contratación?				X	Tanto quien propone el gasto como quien lo autoriza (órgano de contratación) firman la declaración en la memoria justificativa del gasto.
DETECCIÓN					
¿Se han definido indicadores de fraude o señales de alerta y se han comunicado al		X			Hasta el momento, las auditorías son la fuente a través de la cual se puede

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

personal en posición de detectarlos?					detectar el fraude o las conductas corruptas o poco éticas.
¿se utilizan herramientas de análisis de datos o de puntuación de los riesgos?		X			
¿Hay habilitado algún canal de denuncia para cualquiera que detecte una situación de fraude?	X				Aunque no hay canal habilitado para ello, hasta ahora no se ha producido ninguna denuncia ni interna ni externa.
¿Hay alguna unidad o departamento encargado de examinar las denuncias y proponer medidas?	X				No existe formalmente.
CORRECCIÓN					
¿Se evalúa la incidencia del fraude y se califica como puntual o sistémico?	X				No se han producido casos de fraude o corrupción que haya habido que corregir en las últimas dos legislaturas (con la actual DG).
¿Se comunican los hechos y las medidas adoptadas a la autoridad responsable según proceda?	X				
¿Se denuncian los hechos a las autoridades públicas o ante la fiscalía o los tribunales competentes?	X				
Subtotal Puntos	6	12	6	8	
Puntos totales	32				
Puntos máximos	64				
Puntos relativos (totales/máximos)	50%				

En cuanto a la situación actual de protección ante posibles ciberataques (ciberseguridad) se analizan los siguientes aspectos:

*Puntuación: 1 (no), 2 (parcial), 3 (habitual), 4 (sí)

	Grado de cumplimiento				Justificación
CIBERSEGURIDAD	1	2	3	4	
¿Existe un sistema integral de protección de los archivos de uso diario de la FCVRE?				X	Los PC de Alicante y Valencia y su contenido están protegidos por el sistema de la GVA, a través de la DGTIC. Los PC de Bruselas por un sistema de firewall y antivirus que se renueva cada año y que es gestionado por una empresa de mantenimiento IT belga.
¿Existen medias de seguridad como programas de gestión de contraseñas, doble factor de autenticación para transferencias, etc.?	X				No existen estas medidas de seguridad.
¿Se imparte formación al personal de la FCVRE sobre las medidas de seguridad a adoptar para evitar ciberataques y fuga de información?		X			La técnica de gestión financiera recibe formación periódica por la DGTIC, el resto de personal no.
Subtotal Puntos	1	2	0	4	
Puntos totales	7				
Puntos máximos	12				
Puntos relativos (totales/máximos)	58,33%				

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

6. DECLARACIÓN INSTITUCIONAL

Como parte integrante de este plan, el anexo I hace referencia a una declaración institucional de la dirección de la FCVRE y de su patronato de compromiso frente al fraude, la corrupción y los conflictos de interés.

7. MEDIDAS Y ACCIONES CONTRA EL FRAUDE Y LOS CONFLICTOS DE INTERÉS

7.1. Medidas de prevención.

La FCVRE implementará las siguientes medidas de prevención del fraude y los conflictos de interés en las que implicará al personal de la entidad y a su dirección. Concretamente:

7.1.1. Concienciación y desarrollo de una cultura ética entre el personal de la entidad.

- **Difusión del plan entre el personal de la FCVRE.** El presente plan tiene como finalidad principal sistematizar y facilitar el conocimiento del marco normativo y el código de conducta aplicable a los altos cargos (dirección) y a las personas empleadas por la FCVRE, así como formalizar los compromisos adicionales que asume la FCVRE en la lucha contra el fraude.

Responsable de la medida	La dirección y el/la técnico de gestión financiera y administrativa.
Plazo de ejecución	Una semana desde la aprobación del plan por el Patronato y cada vez que se produzca su revisión y evaluación.

- **Análisis y detección de las necesidades de formación en materia de lucha contra el fraude.** Se realizará un análisis para la detección de las necesidades de formación en los centros de trabajo de la FCVRE (Alicante, Bruselas y Valencia) directamente relacionadas con la gestión de expedientes de índole financiera y/o gestión de documentos con información sensible.

Responsable de la medida	La dirección y el/la técnico de gestión financiera y administrativa (responsable de la gestión del personal).
Plazo de ejecución	Dos meses desde la aprobación del plan por el Patronato.

7.1.2. Prevención de conflictos de interés.

- **Declaración de ausencia de conflicto de interés.** Será obligatoria la subscripción de una declaración de ausencia de conflicto de intereses, según el modelo que se recoge en el Anexo II de este plan, por parte de todas las personas que intervengan en tareas directivas y ejecutivas en los procesos de contratación. Esta declaración deberá suscribirse al inicio de dichos procedimientos. En todo caso, la declaración deberá ser suscrita por:
    - El responsable del órgano de contratación o el que ejerza sus funciones en caso de delegación.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

- El personal que redacte los documentos de la licitación; informes, pliegos, contratos, etc.
- El personal que efectúa la evaluación de las ofertas y propuestas técnicas.
- Los miembros de la mesa de contratación y otros órganos colegiados intervinientes en el procedimiento.
- El personal que redacte las propuestas de adjudicación.
- El personal que se encargue del seguimiento de la ejecución del contrato.

En caso de órganos colegiados, la declaración podrá efectuarse de manera verbal por cada uno sus miembros al inicio de la reunión correspondiente y se reflejará en el acta de la sesión.

Responsable de la medida	La dirección (órgano de contratación) y el/la técnico de gestión financiera y administrativa (gestor/a de la contratación).
Plazo de ejecución	Cada vez que se inicie un procedimiento de contratación.

7.1.3. Compromiso con el plan por parte de los participantes en procedimientos de contratación.

- **Declaración de compromiso con el cumplimiento del Plan.** Todas las personas físicas o jurídicas que participen como licitadoras en los procedimientos de contratación que convoque la FCVRE tendrán que suscribir una declaración que acredite que conocen el contenido de este plan y se comprometen a contribuir al cumplimiento de sus objetivos y medidas. La declaración se tendrá que formalizar conforme al modelo que se recoge en el Anexo III y se incluirá entre los anexos de la licitación a presentar por las empresas licitadoras.

Responsable de la medida	El/la técnico de gestión financiera y administrativa (gestor/a de la contratación).
Plazo de ejecución	Cada vez que se ponga en marcha un procedimiento de contratación.

7.2. Medidas de detección.

La FCVRE implementará las siguientes medidas de detección del fraude y los conflictos de interés en las que implicará al personal de la entidad y a su dirección. Concretamente:

7.2.1. Colaboración con el sistema de alertas para la prevención de irregularidades y malas prácticas (SALER).

El sistema de alertas para la prevención de irregularidades y malas prácticas (sistema SALER) de la Generalitat Valenciana ha sido introducido por la Inspección General de Servicios, que es el organismo interno de control en la Administración de la Generalitat. Sus funciones están definidas por Ley 22/2018, de 6 de noviembre, de la Generalitat, de Inspección General de Servicios y sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental. El artículo 24 de dicha Ley establece su obligación de mantener y aplicar el sistema y asegurar su

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

integridad y la fiabilidad de su funcionamiento. Además, todos los departamentos de la Generalitat y los entres incluidos en el ámbito de aplicación de esta Ley están obligados a colaborar en la aplicación del sistema.
Es objetivo de este plan el contribuir a facilitar a la Inspección General de Servicios el ejercicio de sus funciones como órgano responsable de la gestión del sistema SALER, tanto en la detección de posibles irregularidades, negligencias o situaciones de riesgos de fraude, como, si fuera el caso, en las investigaciones subsiguientes.

Responsable de la medida	La dirección, la coordinación y el/la técnico de gestión financiera y administrativa (gestor/a de la contratación).
Plazo de ejecución	Durante la vigencia del plan.

7.2.2. Catálogo de indicadores de riesgo.
En el Anexo IV del presente plan se concreta un catálogo de indicadores de riesgo para la lucha contra el fraude y la corrupción. La posible presencia de un indicador de riesgo no implica necesariamente la existencia de fraude, pero indica que una determinada área ha de ser objeto de atención específica para descartar o confirmar un fraude potencial.

En los procedimientos de contratación que tramite la FCVRE tendrá que quedar documentada la revisión de los posibles indicadores de riesgo. La revisión se verificará en las diferentes fases del procedimiento, según los indicadores de riesgo que se apliquen en cada una de esas fases. Para ello, se utilizará la lista de comprobación según el siguiente modelo y su resultado se incorporará al expediente correspondiente. En caso de que se detecte la presencia de indicadores de riesgo se aplicará el protocolo para la corrección y persecución de posibles fraudes previsto en este plan.

LISTA DE COMPROBACIÓN DE INDICADORES DE RIESGO DE FRAUDE

Procedimiento: (identificación del expediente)

Indicador de riego (Anexo IV)	*¿Se ha detectado en el procedimiento?*			*Observaciones*	*Medidas a adoptar*
	Si	*No*	*N/A*		

Fecha, firma y nombre de la persona que lo firma.

Responsable de la medida	El/la técnico de gestión financiera y administrativa (gestor/a de la contratación) y la administrativa de Bruselas.
Plazo de ejecución	Durante la vigencia del plan.

7.2.3. Difusión de los canales de denuncia existentes.
La FCVRE difundirá entre su personal los distintos canales de denuncia disponibles para que cualquiera que detecte una irregularidad, fraude o caso de corrupción lo pueda

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

denunciar sin el conocimiento necesario de la dirección de la entidad o del resto de los miembros de la plantilla. Esta relación se deberá actualizar cuando se pongan en funcionamiento nuevos canales de denuncia. Son los siguientes:

Autonómicos:

- Buzón de denuncias ante la Agencia Valenciana Antifraude: https://www.antifraucv.es/buzon-de-denuncias-2/#pll_switcher

- Buzón de denuncias ante la Inspección General de Servicios de la Generalitat. https://www.gva.es/es/inicio/procedimientos?id_proc=19518&version=amp

Estatales:

- Servicio nacional de coordinación antifraude (SNCA): https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/comunicacionsnca.aspx

- Buzón antifraude del Plan de Recuperación, Transformación y Resiliencia: https://planderecuperacion.gob.es/buzon-antifraude-canal-de-denuncias-del-mecanismo-para-la-recuperacion-y-resiliencia

7.2.4. Procedimiento para el tratamiento de posibles conflictos de intereses.

Las distintas opciones que una persona de la organización tiene para denunciar o informar de un posible caso de conflicto de intereses serán:

a) Comunicar a un superior jerárquico por la persona afectada el posible conflicto de interés.
   Cuando exista el riesgo de un conflicto de intereses que implique a un miembro del personal que participe en un procedimiento de contratación, de selección de personal o de cualquier otro tipo, la persona afectada deberá ponerlo en conocimiento de su superior jerárquico.
   Aquellas personas o entidades que tengan conocimiento de un posible conflicto de intereses en cualquier procedimiento de la entidad tendrán que poderlo inmediatamente en conocimiento del órgano de contratación, comisión de selección, etc.
b) Cuando el superior jerárquico reciba la comunicación en este sentido deberá analizar los hechos con la persona afectada para aclarar la situación y confirmará por escrito si se considera que existe un conflicto de intereses. Si es así, tendrá que adoptar las medidas que procedan, como solicitar a la persona afectada su abstención en el procedimiento o si es necesario incluso apartar a esa persona mediante su recusación.
   En el caso en que se haya comunicado al superior jerárquico intentos de los participantes en el procedimiento de adjudicación de contratos de influir indebidamente en el proceso de toma de decisiones o de obtener información confidencial y se disponga de documentación que así lo acredite, se pondrá el caso en conocimiento del órgano de contratación o de selección para la adopción de las medidas que procedan, conforme a la normativa vigente.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

c) En caso de que la situación de conflicto se haya detectado con posterioridad al hecho que haya podido producir sus efectos se aplicará el procedimiento previsto para los supuestos de fraude potencial.
Se documentarán los hechos producidos y se pondrá la situación en conocimiento de la unidad con funciones de control de gestión (la dirección o la coordinación de la entidad), para su valoración objetiva y adopción de medidas oportunas.

7.3. Medidas de corrección y persecución

En el supuesto de que se detecte un posible fraude, o exista sospecha fundada, la entidad correspondiente deberá:

a) Suspender inmediatamente el procedimiento, notificar tal circunstancia en el más breve plazo posible a las autoridades interesadas y a los organismos implicados en la realización de las actuaciones y revisar todos aquellos procedimientos o procesos de selección que hayan podido estar expuestos al mismo.
b) Comunicar los hechos producidos y las medidas adoptadas a la dirección o la coordinación de la entidad, quien comunicará el asunto a la Autoridad Responsable, la cual podrá solicitar la información adicional que considere oportuna de cara a su seguimiento y comunicación a la Autoridad de Control.
c) Denunciar, si fuese el caso, los hechos a las Autoridades competentes, para su valoración y eventual comunicación al Servicio nacional de coordinación antifraude (SNCA).
d) Iniciar una información reservada para depurar responsabilidades o incoar un expediente disciplinario.
e) Denunciar los hechos, en su caso, ante el Ministerio Fiscal, cuando fuera procedente.

Responsable de la medida	La dirección y/o la coordinación de la FCVRE.
Plazo de ejecución	Durante la vigencia del plan.

8. CIBERSEGURIDAD

El Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV) es el departamento de la Generalitat Valenciana que vela por la seguridad en la red. Este departamento difunde distintas guías para informar a los usuarios de internet sobre las amenazas y los errores más comunes que cometen los usuarios de la red, así como las medidas de seguridad y las herramientas que se pueden aplicar para protegerse de estas amenazas. A continuación, se van a relacionar los errores más habituales que se cometen, un glosario de amenazas recurrentes y, por último, una serie de consejos para protegerse de todos los peligros al navegar por internet.

Errores más frecuentes que desprotegen la información al navegar en internet.

ERROR 1: Usar la misma contraseña para acceder a las redes sociales, a la cuenta de banco o a cualquier otra aplicación o plataforma (compras por internet, etc.)

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

PROTECCIÓN: Utilizar un gestor de contraseñas para poder manejarse fácilmente con todas las credenciales de acceso. El CSIRT-CV recomienda KeePass Password Safe (http://keepass.info/). Se trata de la herramienta de software libre para gestión de contraseñas más utilizada, la cual almacena las contraseñas cifrándolas con los métodos de cifrado AES y Twofish. KeePass permite organizar las contraseñas en diferentes carpetas según el tipo de servicio al que den acceso. Permite también añadir direcciones web, notas, e incluso ficheros. Se pueden adjuntar certificados digitales que se quieran proteger, imágenes, o cualquier otro fichero que se vaya a necesitar para acceder a nuestros servicios.

ERROR 2: Conectarse a redes WIFI públicas.

PROTECCIÓN: Hay que evitar conectarse a redes WIFI públicas, sobre todo, si se van a realizar operaciones bancarias. En estas redes abiertas, cualquier ciberdelincuente podría estar espiando la red y robar contraseñas tan importantes como la de acceso a la cuenta bancaria. Si aun así se hace, hay que fijarse que sea siempre a través de HTTPS (el candado cerrado) para que la información vaya cifrada. Y borrar el historial de navegación una vez el dispositivo deje de estar conectado a la red pública.

ERROR 3: Usar contraseñas inseguras. Parece increíble que una de las contraseñas más frecuentes siga siendo 123456. Es un error muy habitual utilizar nombre y año de nacimiento e incluso el nombre de una mascota.

PROTECCIÓN: Una contraseña robusta tiene que tener 8 o más caracteres, mayúsculas y minúsculas, signos de puntuación y caracteres especiales (%, $, &…) y sobre todo, cambiarlas periódicamente, así las cuentas estarán siempre seguras.

ERROR 4: Cuidado con los adjuntos que se reciben por email. Si se recibe un fichero adjunto desde una cuenta desconocida no es conveniente abrirlo, probablemente sea malicioso. Si lo envía un conocido, pero parece “extraño”, conviene consultarle antes de abrirlo.

ERROR 5: No denunciar si se es víctima de un ciberdelito. No hay que pensar que no se puede hacer nada.

PROTECCIÓN: Si han suplantado la propia identidad en redes sociales o en cualquier otro ámbito de la red, hay que denunciarlo lo antes posible. Por otro lado, si se es víctima de un ransomware (secuestro de la información, archivos, etc. de una organización para pedir un rescate) no hay que sucumbir al chantaje y pagar el rescate a los secuestradores para recuperar la información, pues es muy probable que lo vuelvan a hacer. Hay que denunciarlo.

ERROR 6: No mantener la privacidad. Un error muy común es no ser cuidadosos con la información que se maneja en el lugar de trabajo, y eso es algo que puede traer consecuencias nefastas en cualquier carrera profesional.

PROTECCIÓN: Tomar ciertas precauciones como cerrar siempre todas las sesiones de las cuentas de redes sociales o de cualquier otro servicio y si se ausenta un momento, es conveniente bloquear siempre el equipo.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

ERROR 7: No cambiar las contraseñas que vienen por defecto en el rúter de casa o del trabajo.

PROTECCIÓN: hay que cambiarla lo antes posible y para estar protegido en el caso de que ciberdelincuentes consigan acceder a la información de la compañía a la que pertenece el dispositivo. Además, hay que mantener siempre actualizado su firmware. Tanto el cambio de contraseña como la actualización del firmware se debería hacer en cualquier dispositivo que se tenga en casa o en el trabajo.

El CSIRT-CV ofrece cursos gratuitos para formarse en medidas de seguridad ante los ciberataques y en su web hay numeroso material relacionado con las medidas de protección (https://www.csirtcv.gva.es/).

Recomendaciones en el uso de dispositivos portátiles fuera de la oficina (teletrabajo)

Durante la última década se ha observado un descenso de los precios de los equipos y componentes informáticos, lo que ha producido un aumento muy significativo de las ventas de equipos portátiles y después de los dos últimos años, con la pandemia por la COVID-19 el uso de equipos domésticos se ha generalizado aún más entre la población, e incluso en sectores que no estaban familiarizados con ellos.

Estas recomendaciones tienen como objetivo informar de los riegos a aquellos usuarios que consultan su correo electrónico en una cafetería mientras toman un café, ven películas mientras esperan en el aeropuerto, se conectan a una red wifi gratuita o comparten su equipo con todos los miembros de su familia. Es necesario que todos ellos sean conscientes de los peligros que corren y tomen medidas para proteger sus equipos y la información valiosa que tienen en ellos.

1. **Promover la seguridad y controlar nuestra privacidad es importante.** A diario se utilizan muchas aplicaciones y redes sociales que tienen acceso a gran cantidad de información (imágenes, vídeos, datos bancarios…). Entre sus principales peligros se sitúan el robo de identidad, el *spam*, el acoso, el *phishing* o los *malware*. Nadie está exento de sufrir dichos peligros.

Por este motivo, se recomienda disponer siempre de una **copia de seguridad** que nos permita proteger esa información. Los ***backups*** son necesarios para garantizar la recuperación de los datos en caso de ciber incidentes, errores humanos, técnicos o naturales. Las copias de seguridad pueden ser almacenadas en soportes como los discos duros externos, las memorias USB, e incluso, la nube. En el caso de las redes sociales, estas plataformas suelen contar con herramientas y opciones de *backup*.

Para una adecuada gestión de copias de seguridad es necesario tener en cuenta factores como la ubicación, el período de conservación, el cifrado de datos y/o la gestión y destrucción de soportes. Algunos consejos que nos ayudarán a proteger nuestra información son:

- Contar con un plan de copias de seguridad diario.
- Realizar *backups* de forma automática.
- Comprobar periódicamente que se están realizando.
- Duplicar periódicamente las copias diarias a un soporte externo (USB, nube…).

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

2. La protección de la información y los dispositivos es esencial para prosperar en un mundo tan conectado como el actual. **Actualizar el *software*** de los dispositivos, entender cómo navegar de forma segura a través de las redes WIFI públicas, y entrar en webs con el protocolo HTTPS son buenas prácticas destinadas a mantener nuestra información segura.

Es imprescindible que todos los dispositivos cuenten con antivirus de calidad y fiables para detectar *malware* u otros elementos maliciosos, mitigando posibles amenazas y siendo capaces de poner el dispositivo en cuarentena para evitar males mayores. Mantener el *software* antivirus actualizado se convierte en una práctica determinante para seguir estando protegidos.

Los programas antivirus tienen como propósito evitar que nuestro sistema se infecte e identificar cambios que pudieran ser realizados por algún *malware* (programas maliciosos).

Por su parte, existen otras herramientas de seguridad como el *firewall*. Esta herramienta se dedica a escanear los paquetes de red y los bloquea o no según las reglas previamente definidas. Gracias a los *firewalls* se puede inspeccionar el tráfico web, identificar usuarios, y bloquear accesos no autorizados. Existen *firewalls* de todo tipo, de filtrado de paquetes, de *proxy*, *software*, *hardware* o nube.

3. Para proteger nuestro ordenador (u otro dispositivo) del uso no autorizado de otras personas es fundamental establecer **contraseñas** en el sistema operativo (o aplicar un cifrado a un disco duro), evitando el acceso y protegiendo la información contenida.

El bloqueo de acceso al BIOS con contraseña es el primer control de seguridad a implementar en un equipo portátil. La contraseña BIOS es una medida que se debe introducir tanto para prevenir cambios en la configuración del BIOS como en el arranque del sistema. Es imprescindible que esta contraseña sea robusta. Sin la contraseña BIOS, un desconocido no podrá acceder al menú de configuración de inicio del equipo, ni iniciar el sistema operativo.

4. Además de una **contraseña BIOS** como primera medida de seguridad para acceder al equipo, existen otros controles de acceso que se pueden establecer cuando se tiene que iniciar el sistema operativo. Hay varias posibilidades, ya que se pueden implementar controles de acceso más sofisticados que las tradicionales contraseñas. Estos son algunos de ellos:

- Memorias USB utilizadas como contraseña.
- Tarjetas criptográficas.
- Lectores de huella dactilar.
- Sistemas de proximidad.

5. Hay que tener en cuenta que con las contraseñas de acceso se evita que se tenga acceso al BIOS y al arranque del sistema, pero no que se extraiga el disco duro, se coloque en otro equipo y se acceda a la información. Para garantizar que la información que hay en el dispositivo portátil no pueda robarla ni leerla nadie que quiera utilizarla con fines maliciosos, se puede recurrir al cifrado. El **cifrado** es la base principal de la seguridad de

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

datos, y dependiendo de la naturaleza de la información contenida podemos optar por dos opciones:

- Cifrar todo el sistema.
- Cifrar únicamente determinados archivos y datos sensibles.

La mayoría de los sistemas operativos ofrecen la opción de cifrar las carpetas personales de los usuarios de forma nativa.

6. Hay una serie de **herramientas** que nos pueden ayudar a recuperar nuestros dispositivos portátiles en caso de robo. Hoy en día existen varios programas que se ayudan de cámaras web, GPS y redes inalámbricas integradas en los portátiles, de forma que cuando el equipo tiene conectividad a Internet puede enviar a una dirección de correo electrónico capturas de pantalla, fotos tomadas desde la webcam o incluso las coordenadas del GPS marcando la posición en la que se encuentra. Además, algunos dispositivos móviles disponen de herramientas nativas de borrado remoto y/o localización del terminal.

7. Muchas veces se usan los equipos portátiles fuera del puesto de trabajo o del hogar, y es muy posible que haya una conexión a una **WiFi pública**. Conectarse a las redes WIFI públicas y gratuitas es tentador en determinadas circunstancias (aeropuertos, cafeterías, hoteles…), pero los riesgos a los que nos exponemos son altos. Al usarlas se exponen los datos, el tráfico y la identidad de forma casi total.

En caso de que el equipo sea vulnerable, ya sea mediante Bluetooth o Wireless, se estará expuesto a ser víctimas de un ciberataque. Para evitarlo, se recomienda deshabilitar las conexiones inalámbricas en caso de no estar utilizándolas, de esta forma no solo se estará protegiendo el equipo, sino que también se reducirá el consumo de las baterías.

De igual modo, otras buenas recomendaciones son:

- No usar aplicaciones con información sensible si hay versiones web de esos servicios. Por ejemplo, acceder con un navegador a esos servicios –web de Facebook- para garantizar que el protocolo utilizado en esa página sea HTTPS antes de introducir las credenciales.
- Cerrar la sesión de los servicios utilizados para que no quede ningún “resto” de nuestra conexión a esos sitios web.
- Usar VPNs para la protección de las comunicaciones a través de la conexión virtual punto a punto.

8. Muchas veces los equipos de casa son utilizados por todo el entorno familiar. Para estos casos, se recomienda siempre crear **cuentas de usuario** para cada uno de los miembros de la familia *«sin permisos de administrador*» y dejar al usuario administrador solo para tareas de configuración e instalación de aplicaciones.

De esta forma, cada usuario podrá tener su propio escritorio, con una configuración y preferencias personalizadas y, además, se reduce el riesgo de pérdida de información debido a fallos y errores no intencionados. Como existe un entorno aislado para cada

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

usuario, se evitará que, por ejemplo, alguien borre accidentalmente los documentos de trabajo. Pero no solo eso, también se estará más protegido frente a virus, troyanos, etc. ya que si el equipo se infecta mientras se está usando una cuenta de usuario estándar, el impacto será siempre mucho menor.

Además de todas estas ventajas, existen opciones de configuración en las cuentas de usuario cuyo objetivo es incrementar la seguridad de los menores. Para ello es muy útil, por ejemplo, *Microsoft Family Safety*.

9. La **seguridad física** de los dispositivos es vital y tiene por objeto mantener la información a salvo. En este sentido, algunas medidas para proteger el ordenador pueden parecer muy obvias y quizá no se plantea su implantación justamente por eso.

Las medidas de protección del *hardware* están destinadas a mantener la integridad de los dispositivos, periféricos (discos duros, USB…), y el conjunto de elementos físicos o materiales que componen los dispositivos.

Algunas de las medidas que van a ayudar a proteger los dispositivos son:

- No mostrar excesivamente los equipos en lugares públicos, salvo que sea necesario.
- Evitar, preferentemente, los maletines de portátil. Lo mejor es utilizar mochilas o maletines que no induzcan a pensar que contienen equipos portátiles.
- Dejar un número de contacto adherido al portátil. De esta forma, si el equipo es extraviado y encontrado, será posible contactar con el dueño y devolvérselo.
- Bloquear el dispositivo una vez se haya dejado de utilizarlo, o si vamos a ausentarnos momentáneamente.
- No perder de vista los dispositivos en ningún momento. Especialmente en sitios públicos.
- Guardar los dispositivos o aquellos dispositivos de almacenamiento con información sensible, en lugares seguros, sin riesgo de golpes, caídas o temperaturas extremas.
- Configurar el equipo para evitar que se auto ejecuten dispositivos externos como USB.

10. Es posible que se piense que la información que contienen los dispositivos domésticos no es crítica y que no es necesario tomar medidas de seguridad para **salvaguardar los datos** que contienen en ellos, pero muchas veces no tienen en cuenta que en caso de robo perderían información tan valiosa como esta:

- Fotografías y vídeos personales que podrían llegar a ser publicados en Internet, e incluso ser utilizados para extorsionar y chantajear a la víctima del robo bajo la amenaza de que se hagan públicas.
- Ficheros con contraseñas: existen usuarios que almacenan sus contraseñas en ficheros descifrados u hojas de cálculo.
- ” Recordar contraseñas” en navegadores: Muchos usuarios utilizan la opción “recordar contraseña” que tienen los navegadores para no tener que escribir las contraseñas de acceso en los servicios online que más utilizan.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

- Correo electrónico almacenado: si el correo no está cifrado, queda expuesto a ser consultado por usuarios maliciosos.
- Información bancaria que podría ser utilizada para realizar compras por Internet, contratar servicios a cuenta del usuario y realizar movimientos bancarios ilícitos.

Estas medidas de protección se deben aplicar, tanto a los ordenadores portátiles de uso privado, como (y, sobre todo) a los dispositivos pertenecientes a la entidad con los que se trabaja desde los domicilios particulares, ya que desde se accede a información compartida y archivos de la FCVRE.

Cómo proteger el móvil de ciberataques

Recientemente se ha detectado un aumento del 500% en los intentos de envío de *malware* para móviles en Europa. Una tendencia que va en aumento debido al enorme uso de la mensajería móvil. Además, no han sido pocos los programas maliciosos para móviles que han pasado a protagonizar portadas de periódicos en los últimos tiempos, siendo uno de los más recientes el *spyware* **Pegasus**.
Es necesario adoptar medidas para evitar ser víctimas de alguno de estos ciberataques, protegiendo nuestros datos privados o los de las organizaciones en las que trabajamos.

El CSIRT-CV ofrece unos útiles consejos:

1. Refuerzo de la seguridad en tu *smartphone*, sobre todo si se trata de un Android, instalando un programa antivirus. Desde el CSIRT-CV recomiendan buscar siempre soluciones oficiales procedentes de fabricantes reconocidos y de confianza, ya que incluso en las *appstores* oficiales aparecen aplicaciones cuyo objetivo es instalar *malware* en los *smartphones*, evadiendo todos los controles de seguridad existentes en las mismas. Un antivirus actualizado siempre añadirá un nivel de protección adicional. «Malwarebytes» es una opción popular y recomendable, un *software anti-malware* disponible en varias plataformas.

2. Protección del acceso a tu móvil con un PIN, patrón, contraseña y añadiendo un sistema de identificación biométrica (huella, reconocimiento facial, etc.). En caso de que el dispositivo tenga la opción de bloquear y desbloquear con un sistema de identificación biométrico como el reconocimiento facial o la huella dactilar, debe utilizarse siempre. Es un sistema mucho más seguro que únicamente una contraseña. Además, la contraseña puede ser hackeada con más facilidad, sobre todo si su nivel de seguridad es bajo.

3. No deben aplazarse las actualizaciones del sistema operativo ni tampoco las de las aplicaciones que del móvil. Postergar una actualización del sistema operativo de un smartphone compromete seriamente su seguridad. Las actualizaciones del *firmware* y aplicaciones son fundamentales a la hora de evitar ciberriesgos, ya que corrigen vulnerabilidades detectadas y es importante tener siempre instalada la última versión disponible. Lo más sencillo es tener activadas las actualizaciones automáticas, pero también es recomendable hacer comprobaciones manuales de vez en cuando.

4. Descarga de las aplicaciones siempre de los sitios web o de las tiendas oficiales (Google Play o App Store). Debe revisarse quién es el proveedor/fabricante, el número de descargas y los comentarios de otros usuarios, para verificar mejor que la app

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

es segura. También es imprescindible que se revisen los permisos que se conceden antes de instalar las aplicaciones, ya que a veces éstos no son necesarios para su funcionamiento y podrían llegar a ser robados de servidores de terceros y utilizados con fines delictivos.

IMPORTANTE: nunca deben instalarse aplicaciones que no provengan de fuentes de confianza. Es algo que puede parecer evidente, pero a veces, muchas aplicaciones de moda, de las que todo el mundo habla, no están en tiendas oficiales y pueden llegar a ser un verdadero nido de *malware*.

5. Desactivar las opciones de conexión inalámbrica cuando no se necesiten. Existe una tendencia generalizada a tener todo activado, aunque no lo esté en uso y eso es necesario cambiarlo. Si no se está utilizando el wifi, el bluetooth o los servicios de localización, es mejor desactivarlos. Lo mismo debe hacerse con aquellas aplicaciones que no se utilicen a menudo.

Además, debe evitarse siempre conectarse a redes wifis públicas o a aquellas que no tengan una contraseña para conectarse. Teniendo en cuenta estas medidas, se evitará que la información que se encuentra en un dispositivo quede expuesta a cualquier persona que tenga fines maliciosos y quiera robar datos personales.

6. El cifrado de datos es un escudo infalible para evitar que los ciberdelincuentes accedan a móvil. Hacer uso de las capacidades nativas de cifrado del dispositivo ayudará a encriptar toda la información almacenada en él. De esta manera, en caso de robo o pérdida, un tercero no autorizado no podrá acceder a ella. Si el dispositivo es un iPhone, el cifrado está por defecto a partir de iOS 8 y si es un Android, puede comprobarse en Ajustes > Seguridad > Cifrar teléfono. Puede que no aparezca exactamente igual, dependiendo de la versión de Android que se use.

7. Nuestro teléfono móvil nos acompaña prácticamente a todos los sitios, lo que aumenta la probabilidad de robo o extravío. Por eso, desde CSIRT-CV SE recomienda que se active la opción "**encuentra mi móvil**" ya que permitirá bloquearlo e incluso localizarlo. Además, si no se recupera, al menos no accederán al contenido.

Otra práctica que se debería adoptar es la de realizar copias de seguridad periódicas o tener activado algún sistema de **copia de seguridad** automático que permita tener un backup en caso de emergencia y evitar así la pérdida definitiva de la información.

8. Además de tener un antivirus instalado en el móvil, también es recomendable que se disponga de **alguna aplicación que revise su seguridad** y que avise si hay instalada alguna aplicación maliciosa. Se recomienda la utilización de «CONANmobile», una app de Incibe para Android que no solo alerta en caso de detectar alguna aplicación con *malware*, sino que también verifica que están actualizadas todas las aplicaciones y comprueba que la configuración del dispositivo es la correcta.

9. Si se recibe un SMS inesperado o un mensaje de WhatsApp de un número desconocido con **un enlace, NUNCA debe hacerse clic** para así evitar prácticas como el *phishing*. Podría contener un *malware* que se instalaría en el dispositivo y podría, por ejemplo, realizar una suscripción a un servicio de pago. Además, hay que tener cuidado con el *smishing*, ya que muchas veces los ciberdelincuentes envían un SMS suplantando la

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

identidad de una organización legítima con el objetivo de robar información o realizar un cargo económico.

10. Es muy importante reconocer cuándo el móvil está infectado. Hay que sospechar en alguna de estas situaciones:

- El navegador se llena de anuncios.
- Aparecen notificaciones con publicidad en la barra de menú.
- Hay un consumo excesivo de datos o batería o el móvil va muy lento.

Si hay indicios de que el móvil tiene un *malware*, hay que descargar un antivirus para que escanee el dispositivo y elimine las amenazas. Si después de haber hecho esto el problema persiste, la opción más segura es restaurar los valores de fábrica del dispositivo.

Consejos para no ser víctima del fraude del ceo (de las siglas en inglés de chief executive *officer*, director ejecutivo en castellano).

Dado el aumento de casos relacionados con el fraude del CEO que se están produciendo en los últimos meses, desde CSIRT-CV se ofrecen 10 consejos para no ser víctima de un fraude del CEO, con el objetivo de intentar no caer en esta estafa. Este tipo de engaño consiste en hacer llegar un correo, remitido supuestamente por un superior de la organización, a un empleado o empleada que tenga la posibilidad de realizar transferencias o acceder a datos de cuentas, presionándole para realizar alguna operación financiera e indicándole que es confidencial y urgente.

Con esta campaña se pretende destacar la importancia de concienciar a todos los empleados, tanto de organizaciones públicas como privadas, para no ser víctimas de estos engaños. Los miembros de la organización deberían ser la primera barrera ante estos timos, los cuales cada vez son más difíciles de detectar. Últimamente, los casos descubiertos estaban perfectamente organizados y los correos eran muy creíbles dado el nivel de detalle que presentaban.

Desde CSIRT-CV se recomienda seguir los siguientes consejos:

1. El objetivo principal de los ciberdelincuentes que quieren llevar a cabo el *Fraude del CEO*, son los empleados de las organizaciones que tienen acceso a datos de las cuentas o la potestad de realizar transferencias. Suelen recibir un correo suplantando la identidad de un superior de su organización.

Es muy importante que, si un empleado recibe un e-mail solicitándole una transferencia "urgente", compruebe el dominio del remitente y se asegure que esa dirección coincide exactamente con la cuenta de correo electrónico (nombre y dominio) que corresponde, puesto que los ciberdelincuentes suelen realizar pequeños cambios que pasan desapercibidos. Hay que fijarse muy bien para detectarlos y evitar caer en este engaño.

2. Las campañas más sofisticadas del *Fraude del CEO* suelen venir precedidas de una fase de investigación, en la que el atacante recaba información sobre la estructura orgánica y funcional del organismo o la empresa a atacar, con el fin de dirigirse a la persona adecuada.

Previo al correo de la propia estafa, la empresa u organismo pueden haber recibido diferentes correos electrónicos, cartas postales y/o llamadas telefónicas **solicitando**

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

información sobre personas de contacto, facturas, cobros y contratos, que más adelante serán utilizados para diseñar e hilar la estafa.

Además de basarse en engaños para obtener información veraz, los estafadores también utilizan fuentes públicas como la Plataforma de Contratación del Estado, noticias en prensa o webs oficiales donde se publiquen concursos públicos para conseguir toda la información posible sobre los contratos y organismos relacionados con su víctima.

3. Normalmente, en el *Fraude del CEO* se solicita por e-mail la realización de transferencias o cobros a la organización, con carácter confidencial y urgente, porque los ciberdelincuentes quieren dar el menor tiempo posible a la víctima para evitar ser descubiertos. Además, los atacantes **suelen crear documentos falsificados que incluyen membretes oficiales, firmas escaneadas e incluso firmas digitales falsificadas**, que resultan **extremadamente creíbles** por la persona que es objeto de este engaño. En ocasiones, este tipo de correo electrónico fraudulento también incluye archivos adjuntos. Recuerde, que no se debe abrir ningún archivo adjunto si no conoce al remitente o no espera ningún documento.

4. Si observa alguna anomalía en un correo electrónico, algún detalle que se salga de los procedimientos habituales de su organización y que le haga dudar sobre la veracidad del contenido del e-mail, contacte con el remitente real a través de otro canal (ej. vía telefónica) para comprobar la autenticidad del mensaje. También es necesario disponer de procedimientos robustos, como la exigencia de firma digital o el establecimiento de doble firma para los importes que superen cierta cantidad, ya que siempre resultará más difícil que fructifique un engaño en dos personas que solo en una. La doble verificación es fundamental para evitar el *Fraude del CEO*.

5. Desconfíe siempre de los correos electrónicos cuyo texto esté mal redactado o con faltas de ortografía. Suelen ser frecuentes en este tipo de ataques. Además, en las campañas de *Fraude del CEO* se debe evitar pulsar en cualquier enlace presente en el e-mail, así como abrir documentos de procedencia incierta y, sobre todo, nunca se debe enviar las credenciales de acceso (usuario y contraseña) mediante correo electrónico A NADIE.

6. Para evitar caer en el *Fraude del CEO* hay que prestar siempre especial atención a la sintaxis de los enlaces a páginas web que lleguen por correo electrónico. Una letra puede marcar la diferencia. Tampoco se deben introducir datos personales en páginas web cuyo enlace se haya acortado (cort.as, bit.ly, etc.).

7. En el *Fraude del CEO* las peticiones no se limitan a solicitar directamente el pago de una cantidad económica, sino que abarcan una amplia casuística:

- Solicitud del cobro de facturas sin pagar.
- Atender a transacciones económicas "*con discreción*", "*habiendo depositado mi confianza personal en usted*" o exigiendo mantener el secreto por tratarse de "*movimientos estratégicos para la organización*".
- Solicitud de cambio de cuentas bancarias para futuros pagos.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

- Solicitud de cambio de contactos o direcciones de correo que van a gestionar los pagos en adelante.

- Cambios en la cantidad, alcance o cuantía de servicios contratados.

- Avisos de cambio de resultados en procesos de adjudicación.

- Solicitudes de transferencias **urgentes** por encontrarse el responsable habitual fuera de la oficina o con problemas técnicos para contactar.

Hay que permanecer siempre alerta y notificar cualquier sospecha a *csirtcv@gva.es*

8. Hay que prestar mucha atención a las propuestas de cambio de cuenta bancaria que se reciben por correo electrónico, porque se puede tratar del *Fraude del CEO*. Si se necesita realizar una llamada de verificación hay que hacerla siempre de una manera segura; nunca se debe llamar a un número de teléfono que figure en el e-mail sospechoso, sino al que tengamos en nuestra base de datos corporativa o el que figure en la página web oficial de la entidad a la que supuestamente están intentando suplantar.

9. Si se ha localizado un e-mail sospechoso y se cree que tras él se esconde un *Fraude del CEO*, se recomienda guardar un registro de todos los correos enviados y recibidos, por si se requiere hacer una investigación posterior o formular una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, y mantener una política de contraseñas robustas entre los empleados de la organización.

También queremos recordar que, para cometer este delito, a veces no solo se ha utilizado el correo electrónico, sino que se han recibido **mensajes de texto, llamadas de teléfono o información por correo postal,** como parte del engaño.

10. Para no ser víctima del *Fraude del CEO* lo más importante es NO dejarse intimidar por solicitudes urgentes o amenazantes: los atacantes pueden ser muy persuasivos y pueden hacer creer a la víctima que se trata de un superior o que su puesto de trabajo corre peligro. Además, no hay que olvidar que la mayoría de las veces, los atacantes **crean documentos falsificados que resultan extremadamente creíbles**.

Desde CSIRT-CV se recomienda que, una vez se detecte un e-mail de este tipo, además de proceder a la notificación, se bloquee al remitente en los servidores de correo, para evitar recibir más en el futuro y comprobar que no se han recibido también en cuentas de otros usuarios.

Como conclusión, para no ser víctimas de este tipo de ataques, hace falta trabajar desde una triple perspectiva:

1. Hay que concienciar tanto a empleados públicos como privados. Su educación y capacitación en temas vinculados a la ciberseguridad resultan cruciales.

2. Mejorar la robustez de los procedimientos que tienen que ver con el alta a terceros y la toma de decisiones. Todos los departamentos deben tener protocolos de transacciones financieras claros y sólidos, y cumplirse estrictamente en todos los casos.

3. Contactar con CSIRT-CV (csirtcv@gva.es) ante cualquier sospecha de estar sufriendo un tipo de estafa como esta.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

9. APROBACIÓN, SEGUIMIENTO Y REVISIÓN DEL PLAN.

La aprobación de este plan corresponde al órgano de gobierno de la FCVRE, es decir, su Patronato. La interpretación e impulso de su ejecución y actualización corresponde a la persona que ostente el cargo de dirección, que llevará a cabo dicha misión con el apoyo de los miembros de la plantilla que ocupen los puestos de la coordinación y de técnico de gestión administrativa y financiera. También intervendrá la persona que ocupe el puesto de administrativo/a en Bruselas.

El seguimiento del cumplimiento de las medias del presente plan se realizará por las personas responsables de cada procedimiento que se realice, ya sea un procedimiento de contratación, de selección de personal, etc.

Anualmente se realizará un informe de seguimiento y evaluación de la aplicación del plan que identificará las medias puestas en marcha y las necesidades de mejora o actualización. Este informe se realizará cada mes de diciembre y se informará del mismo al Patronato en la junta ordinaria prevista a final de año.

10. ANEXOS.

- Anexo I: Declaración institucional de compromiso contra el fraude, la corrupción y el conflicto de interés. Patronato de XX de diciembre de 2022.
- Anexo II: Declaración de ausencia de conflicto de interés.
- Anexo III. Declaración de compromiso con el cumplimiento del Plan para empresas licitadoras.
- Anexo IV: Indicadores de riesgo.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

Anexo I

DECLARACIÓN INSTITUCIONAL DE LA FUNDACIÓ COMUNITAT VALENCIANA-REGIÓ EUROPEA

La Fundació Comunitat Valenciana-Regió Europea reitera su compromiso con los estándares más altos en el cumplimiento de las normas jurídicas, éticas y morales, y su adhesión a los más estrictos principios de integridad, objetividad y honestidad, de manera que toda su actividad sea percibida por todos los agentes que se relacionan con ella como opuesta al fraude y la corrupción en cualquiera de sus formas. El personal de la Fundació Comunitat Valenciana-Regió Europea, en su calidad de empleados y empleadas laborales, asumen y comparten este compromiso, teniendo entre otros deberes el de velar por los intereses generales, con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico, y actuar conforme a los siguientes principios: objetividad, integridad, neutralidad, responsabilidad, imparcialidad, confidencialidad, dedicación al servicio público, transparencia, ejemplaridad, austeridad, accesibilidad, eficacia, honradez, promoción del entorno cultural y medioambiental y respeto de la igualdad entre hombres y mujeres.

Para hacer efectivo este compromiso, la Fundació Comunitat Valenciana-Regió Europea aplicará cuantas medidas sean eficaces y proporcionadas para prevenir y detectar los actos de fraude y para perseguirlos y corregir su impacto en caso de que lleguen a producirse.

Secretario de la FCVRE
Ilmo. D. Joan Calabuig Rull

Presidente de la FCVRE
MHP Ximo Puig Ferrer

Directora de la FCVRE
Dª. Daría Terrádez Salom

.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

Anexo II

MODELO DE DECLARACIÓN DE AUSENCIA DE CONFLICTO DE INTERÉS (DACI)

Cada una de las personas que intervienen en un procedimiento de contratación o en un proceso de selección, conforme a lo que prevé el apartado 7.1.2. del Plan de medidas para la prevención del fraude, el conflicto de intereses y la ciberseguridad, deberá firmar la siguiente declaración de ausencia de conflicto de interés:

Expediente: (identificación del expediente de contratación o proceso de selección)

Con el fin de garantizar la imparcialidad en el procedimiento de contratación/selección, arriba referenciado, el abajo firmante, como participante en el proceso de preparación, tramitación, resolución y seguimiento del expediente, declara:

Primero. Estar informado de lo siguiente:

1. Que el artículo 61.3. del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio (Reglamento financiero de la UE), establece que "*existirá conflicto de intereses cuando el ejercicio imparcial y objetivo de las funciones se vea comprometido por razones familiares, afectivas, de afinidad política o nacional, de interés económico o por cualquier motivo directo o indirecto de interés personal*".
2. Que el artículo 64, de la Ley 9/2017, de 8 de noviembre, de contratos del sector público, tiene el fin de evitar cualquier distorsión de la competencia y garantizar la transparencia en el procedimiento y asegurar la igualdad de trato a todos los candidatos y licitadores.
3. Que el artículo 23 de la Ley 40/2015, de 1 de octubre, del régimen jurídico del sector público, establece que deberán abstenerse de intervenir en el procedimiento "*las autoridades y el personal al servicio de las administraciones en los que se dan algunas de las circunstancias señaladas en el apartado siguiente*", siendo estas:
    a. Tener interés personal en el asunto de que se trate o en otro cuya resolución pudiera influir la de aquel; ser administrador de sociedad o entidad interesada, o tener cuestión litigiosa pendiente con algún interesado.
    b. Tener un vínculo matrimonial o situación asimilable y el parentesco de consanguineidad dentro del cuarto grado o de afinidad dentro del segundo, con cualquiera de los interesados, con los administradores de entidades o sociedades interesadas y también con los asesores, representantes legales o mandatarios que intervengan en el procedimiento, así como compartir despacho profesional o estar asociado con estos para el asesoramiento, la representación o el mandato.
    c. Tener amistar íntima o enemistad manifiesta con laguna de las personas indicadas en el apartado anterior.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

d. Haber intervenido como perito o como testigo en el procedimiento de que se trate.
e. Tener relación de servicio con persona natural o jurídica interesada directamente en el asunto, o haberle prestado en los dos últimos años servicios profesionales de cualquier tipo y en cualquier circunstancia o lugar.

Segundo. Que no se encuentra incurso en ninguna situación que pueda calificarse de conflicto de intereses de las indicadas en el artículo 61.3. del Reglamento Financiero de la UE, que no concurra en su persona ninguna causa de abstención del artículo 23.2. de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, que pueda afectar al procedimiento de licitación/selección.

Tercero. Que se compromete a poner en conocimiento del órgano competente para la resolución del expediente, sin dilación, cualquier situación que en adelante pueda dar lugar a la aparición de un conflicto de intereses o causa de abstención.

Cuarto. Es sabedor del hecho que una declaración de ausencia de conflicto de intereses que se demuestra que ha sido emitida de forma deliberadamente falsa, implicará las consecuencias disciplinarias, administrativas o judiciales que establezca la normativa de aplicación.

Fecha, firma, nombre completo y DNI.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

Anexo III

DECLARACIÓN DE COMPROMISO CON EL CUMPLIMIENTO DE LOS OBJETIVOS Y MEDIDAS DEL PLAN

Cada una de las personas que deseen participar en un procedimiento de contratación o de selección de personal, conforme a lo que se prevé en el apartado 7.1.3. de este plan, habrá de firmar la siguiente declaración:

Expediente: identificación del expediente de contratación o selección.

El abajo firmante, en nombre propio/en representación de la entidad …… Con NIF …….. y domicilio fiscal en ……, declara:

Primero. Que desea participar como licitador en el procedimiento de contratación/participante en le proceso de selección arriba referenciado, convocado por la Fundació Comunitat Valenciana-Regió Europea.

Segundo. Que conoce plenamente el contenido de la licitación/las condiciones de la convocatoria de selección publicada por la Fundació Comunitat Valenciana-Regió Europea en su página web www.ue.gva.es/en la Plataforma de Contratación del Estado/en el DOGV en fecha ……

Tercero. Que tanto en las fases de tramitación del procedimiento en las que participo como licitador/candidato/a, como en las fases de ejecución y fiscalización en caso de que resulte adjudicatario del contrato, me comprometo a:

a) Contribuir plenamente a la mejor realización de los principios y objetivos el Plan de Medidas para la prevención del fraude, el conflicto de intereses y la ciberseguridad de la Fundació Comunitat Valenciana-Regió Europea.
b) Adoptar todas las medidas que sean necesarias para hacer efectivo el cumplimiento de las medidas de lucha contra el fraude y de erradicación de los conflictos de interés previstas en el Plan.
c) Garantizar que su actuación en la ejecución del objeto de contrato se llevará a término en todo momento de acuerdo con los intereses financieros de la FCVRE.

Fecha, firma, nombre completo y DNI.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

Anexo IV

INDICADORES DE RIESGO

CONTRATACIÓN

A) PLIEGOS FALSEADOS A FAVOR DE UN LICITADOR.

1. Se ha presentado una única oferta o el número de licitadores es anormalmente bajo.
2. Existe una similitud constatable entre los pliegos del procedimiento de contratación y los servicios y/o productos del contratista adjudicatario.
3. Se ha recibido quejas en este sentido por parte de los licitadores.
4. Los pliegos del procedimiento de contratación incluyen prescripciones que son muy distintas de las aprobadas en procedimientos previos similares.
5. Los pliegos incorporan cláusulas inusuales o poco razonables.
6. El poder adjudicador está definiendo una marca concreta, en lugar de un producto genérico.
7. Ausencia de medidas de información y publicidad en la documentación relativa al procedimiento de contratación y/o insuficiencia de plazo para la recepción de ofertas.

B) COLUSIÓN EN LA LICITACIÓN.

1. El resultado de la licitación lleva a la adjudicación del contrato a una oferta excesivamente alta en comparación con los costes previstos, con las listas de precios públicos, con obras o servicios similares o medios de la industria o con precios de referencia del mercado.
2. Todas las ofertas presentadas incluyen precios elevados de forma continuada. Esto constataría posibles acuerdos entre los licitadores en los precios ofrecidos.
3. Ante la presencia de nuevos licitadores, las ofertas bajan considerablemente.
4. Los adjudicatarios alternan su participación por región, tipo de trabajo, tipo de obra, etc. Constataría posibles acuerdos entre los licitadores para repartirse el mercado.
5. Existen subcontratistas que participaron en la licitación.
6. Existen patrones de ofertas inusuales (por ejemplo, se ofrece exactamente el presupuesto del contrato, los precios de las ofertas son demasiado altos, demasiado próximos, etc.)
7. Evidencia de conexiones entre los licitadores (por ejemplo, domicilios comunes, personal, números de teléfono, etc.)
8. El contratista comunica a subcontratistas que también participan como licitadores.
9. Compiten siempre unas ciertas compañías y otras no lo hacen nunca.
10. Existen licitadores ficticios.
11. Evidencia de que ciertos licitadores intercambian información, obteniendo así cuerdos informales.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

C) CONFLICTO DE INTERESES.

1. Se favorece a un contratista o vendedor en concreto, sin ninguna explicación o de forma inusual y/o existe un comportamiento inusual por parte de un/a empleado/a para obtener información sobre un procedimiento del que no está al cargo.
2. Algún miembro del órgano de contratación ha trabajado para una empresa que participa en la licitación de forma inmediatamente anterior a su incorporación al puesto de trabajo en el citado organismo de adjudicación.
3. Existe algún vínculo familiar entre un/a empleado/a del órgano de contratación y algún licitador.
4. Se producen reiteraciones en las adjudicaciones a favor de un mismo licitador.
5. Se aceptan precios altos y trabajos de baja calidad.
6. No se presenta la DACI por las personas empleadas encargadas de la contratación o se hace de manera incompleta.
7. La persona encargada de la contratación no acepta un ascenso que supone abandonar los procesos de contratación.
8. La persona empleada participante en la contratación hace negocios propios.
9. Existe relación social más allá de le estrictamente profesional entre la persona empleada que participa en el proceso de contratación y un proveedor de servicios o productos.
10. Inexplicablemente se ha incrementado la riqueza o el nivel de vida de la persona empleada que participa en la contratación.

D) MANIPULACIÓN DE LAS OFERTAS PRESENTADAS.

1. Han existido quejas (denuncias, reclamaciones, etc.) de licitadores.
2. Existe una falta de control y/o inadecuación de los procedimientos de licitación.
3. Hay indicios que evidencian cambios en las ofertas después de la recepción de estas.
4. Existen ofertas que han sido excluidas por la existencia de errores.
5. Hay licitadores capacitados que han sido descartados por razones dudosas.
6. Se han recibido menos ofertas que el número mínimo requerido y aún así se sigue con el procedimiento, sin declararse desierto. O bien se ha declarado desierto el procedimiento y vuelve a convocarse a pesar de recibir ofertas admisibles de acuerdo con los criterios que figuran en los pliegos.

E) FRACCIONAMIENTO DEL GASTO.

1. Se aprecian dos o más adquisiciones con objeto similar efectuadas a favor del mismo adjudicatario, con la única finalidad de no utilizar procedimientos con mayores garantías de concurrencia.
2. Las compras se han separado injustificadamente, por ejemplo, contratos separados de mano de obra y materiales, estando ambos por debajo de los límites de la licitación abierta.
3. Existen compras secuenciales por debajo de los límites de obligación de publicidad de las licitaciones.

C/ Caballeros, 9
46001 Valencia
Tel. +34 96 386 82 02
www.ue.gva.es

F) MEZCLA DE CONTRATOS.

1. Hay facturas similares presentadas en diferentes trabajos o contratos.
2. El contratista factura más de un trabajo en el mismo periodo de tiempo.

G) CARGA ERRÓNEA DE COSTES.

1. Las cargas laborales son excesivas o inusuales.
2. Las cargas laborales son incompatibles con la situación del contrato.
3. Hay cambios aparentes en las hojas de control del tiempo.
4. Inexistencia de hojas de control del tiempo.
5. Hay costes materiales idénticos imputados a más de un contrato.
6. Se imputan costes indirectos como costes directos.

PROCESOS DE SELECCIÓN.

A) LIMITACION DE LA CONCURRENCIA.

1. Falta de suficiente difusión de la convocatoria, incumpliéndose el principio de publicidad y transparencia.
2. Falta una definición clara en la convocatoria de los requisitos que han de cumplir las personas candidatas del proceso de selección.
3. Inobservancia de los términos establecidos en la convocatoria para la presentación de candidaturas.
4. Se produce la ausencia de la publicación de los baremos en los Boletines Oficiales correspondientes.

B) TRATO DISCRIMINATORIO EN LA SELECCIÓN DE LAS CANDIDATURAS.

1. Se incumplen los principios de objetividad, igualdad y no discriminación en la selección de candidaturas. No se sigue un criterio homogéneo para la selección de candidaturas.

C) CONFLICTO DE INTERESES EN EL COMITÉ DE SELECCIÓN.

1. Se ha influido de manera deliberada en la selección de las personas candidatas, favoreciendo a algunos de ellos, dando trato preferente o presionando a otros miembros del comité.

D) FALSEDAD DOCUMENTAL.

1. Se constata la existencia de documentos o declaraciones falsas presentadas por las personas candidatas con el fin de salir elegidas en el proceso de selección.