INSTRUCCIONES:

El siguiente cuestionario pretende articular el alcance de la revisión preliminar sobre los controles más directamente relacionados con la ciberseguridad y cumplimiento de la legalidad en los sistemas de información de la entidad, enmarcado dentro de las actividades de planificación de la auditoría que se está llevando a cabo.

Para cumplimentar el cuestionario no es necesario que se genere documentación adicional a la ya disponible. La idea es la de disponer de la documentación ya existente en la entidad en el momento de inicio del trabajo de campo, con el fin de optimizar el tiempo invertido por ambas partes.

El trabajo de campo se desarrollará principalmente mediante entrevistas, de las que podrán surgir necesidades adicionales de información.

En el caso de que exista documentación descriptiva de los procedimientos, no es necesaria la cumplimentación del cuestionario respecto a esos aspectos, basta con la aportación del documento descriptivo.

Del mismo modo, no es imprescindible que nos facilite aquella información que considere puede ser de carácter confidencial. En esos casos indíquelo en el cuestionario y prepárela para el inicio del trabajo.

El alcance de la revisión posee un carácter general, no siendo necesario obtener una información exhaustiva de cada uno de los puntos incluidos en el cuestionario.

Para cualquier duda, no dude en ponerse en contacto con los miembros del equipo de fiscalización (Correo electrónico: XXX@xx.xx, tf. xxx).

Le rogamos nos facilite el cuestionario cumplimentado lo antes posible.

Una vez cumplimentado se devolverá como un documento ***.docx o *.pdf firmado electrónicamente (preferentemente) o en soporte papel con firma hológrafa del responsable del área de sistemas de información.**

CUMPLIMENTADO POR:

Entidad:

Denominación del Departamento TI:

Nombre:

Cargo:

Fecha:

Firma:

Domicilio del Departamento TI:

INFORMACIÓN GENERAL SOBRE EL ENTORNO TECNOLÓGICO DE LA ENTIDAD

Documentación necesaria:

- Copia del mapa de red
- Diagramas de la arquitectura física/lógica de los sistemas de información de la Entidad

En caso de no disponer de dicha documentación, incluir una breve explicación del entorno de TI de la Entidad (existencia o no de DMZ, de segmentación entre red de usuarios y red de servidores, elementos de seguridad (firewall, IPS, etc.), relación de los principales sistemas ubicados en la red interna, uso de soluciones de virtualización, etc.).

CBCS 1: INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS

1-1: Inventario de activos físicos autorizados

- ¿Existe un inventario de hardware? En caso afirmativo:
  - ¿Proporciona información sobre los siguientes aspectos de cada elemento?
    - Identificación del activo: fabricante, modelo, número de serie
    - Configuración del activo: perfil, política, software instalado
    - Software instalado: fabricante, producto, versión y parches aplicados
    - Equipamiento de red: MAC, IP asignada (o rango)
    - Ubicación del activo: ¿dónde está?
    - Propiedad del activo: persona responsable del mismo
- ¿Está actualizado? Indicar la fecha de última actualización.
- ¿Dispone de una herramienta automatizada que permite la actualización continua del inventario? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
- Si no se dispone de herramienta, indicar cómo se lleva a cabo la actualización del inventario.
- ¿Dispone de un procedimiento de autorización de los elementos hardware antes de su entrada en producción? ¿Está aprobado? ¿Quién lo ha aprobado?

1-2: Control de activos físicos no autorizados

- ¿Dispone de mecanismos para controlar (detectar o restringir) el acceso de dispositivos físicos no autorizados (ej. 802.1x)?
- En caso contrario, ¿cómo garantiza que únicamente se conectan a la red los dispositivos autorizados?

Documentación necesaria:

- Copia del procedimiento de mantenimiento y gestión del inventario de hardware
- Copia del inventario de hardware
- Copia del procedimiento de autorización de hardware
- Copia del procedimiento donde se describan los controles para detectar o restringir el acceso de dispositivos físicos no autorizados.

CBCS 2: INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO

2-1: Inventario de SW autorizado

- ¿Existe una lista actualizada de software autorizado?
- ¿Existe un inventario de software instalado en los dispositivos de la entidad?

  En caso afirmativo, ¿está actualizado? Indicar la fecha de última actualización.
- ¿Dispone de una herramienta automatizada para la gestión del inventario de software?

  En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
- ¿El inventario de hardware y el de software están relacionados? (es decir, para un dispositivo hardware es posible consultar el software que tiene instalado).
- ¿Existe un procedimemiento de autorización de software?

2-2: SW soportado por el fabricante.

- ¿Dispone de un plan de mantenimiento del software, de acuerdo con las especificaciones de los fabricantes?
- El plan de mantenimiento anterior, ¿incluye el control de las fechas de fin de soporte del HW y SW por parte de los fabricantes?
- ¿Existe software fuera de soporte por parte del fabricante? En caso afirmativo, indicar producto, fabricante y versión.

2-3: Control de SW no autorizado

- ¿Se dispone de guías de instalación y bastionado de los sistemas previo a su entrada en operación?
- Las guías de configuración anteriores, ¿ incluyen el detalle del SW a instalar por tipo de sistema y/o usuario? (ej. SW a instalar en el equipo cliente de un usuario no administrador del área de gestión presupuestaria, SW a instalar en el servidor de BBDD de la aplicación X, etc.).
- ¿Dispone de alguna herramienta para controlar e impedir la instalación de software no autorizado (ej.applocker)? En caso afirmativo:
  - Indicar nombre de la herramienta, fabricante y versión.
  - ¿La herramienta detecta automáticamente el software instalado en cada sistema?¿Actualiza de forma automática el inventario de software?
- En caso contrario, ¿existe un procedimiento para la revisión del software instalado en los equipos de la entidad? En caso de detectar software no autorizado en estas revisiones, ¿se elimina?

Documentación necesaria:

- Copia del procedimiento de mantenimiento y gestión del inventario de software
- Copia del inventario de software
- Copia del procedimiento de autorización de software
- Copia del procedimiento/guías de configuración que indique los criterios para la instalación de software según el perfil de sistema y/o usuario.
- Copia del procedimiento de revisión del software instalado en los sistemas de la entidad.

CBCS 3: PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

3-1 Identificación de vulnerabilidades

- ¿Se dispone de una herramienta para la identificación de las vulnerabilidades de seguridad que puedan afectar a los productos y tecnologías de sistemas de información existentes en la entidad?
- ¿Se efectúa un seguimiento continuo de los anuncios de defectos realizados por los fabricantes? ¿Cómo (ej. contratación de un servicio específico a fabricantes, suscripción a listas públicas de publicación de defectos, etc.)? ¿Quién es el responsable de realizarlo?
- Tras la puesta en servicio de un sistema, ¿se realizan análisis de vulnerabilidades periódicos?

3-2 Priorización de vulnerabilidades

- ¿Dispone de un procedimiento para analizar y priorizar la resolución de las vulnerabilidades y defectos de seguridad identificados, basado en la gestión de riesgos?
- ¿El procedimiento anterior define plazos máximos de resolución de las vulnerabilidades en función del riesgo asociado?

3-3 Resolución de vulnerabilidades

- ¿Se realiza el seguimiento de la corrección de las vulnerabilidades identificadas que, de acuerdo a la gestión de riesgos, se ha decidido resolver?

3-4 Parcheo

- ¿Se dispone de un procedimiento para el parcheo de sistemas/tecnologías (sistemas operativos, bases de datos, aplicaciones…)?
- ¿Se dispone de una/s herramienta/s para la gestión e instalación de parches y actualizaciones de seguridad? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.

  En caso de utilizar herramientas diferentes en función de la tecnología, detallar de forma separada cada una de ellas.

Documentación necesaria:

- Copia del procedimiento (o procedimientos) de:
  - Identificación de vulnerabilidades.
  - Análisis y priorización de vulnerabilidades.
  - Seguimiento de la resolución de vulnerabilidades
  - Parcheo de sistemas/tecnologías.

CBCS 4: USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

4-1 Inventario y control de cuentas de administración

- ¿Existe un procedimiento de gestión de privilegios que contemple la limitación de los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?

  En particular, ¿el procedimiento anterior garantiza que se restringen los permisos de administración a los casos en que sea necesario y que sólo se utilicen las cuentas de administrador cuando sea necesario?
- ¿Se dispone de un inventario de las cuentas de administración que permita su adecuada gestión y control?
- ¿Los usuarios que no realizan funciones técnicas son administradores de sus equipos?

4-2 Cambio de contraseñas por defecto

- Antes de la puesta en producción de un sistema, ¿se eliminan/renombran las cuentas de administración estándar y se les cambia la contraseña por defecto?

4-3 Uso dedicado de cuentas de administración

- ¿Los usuarios que disponen de cuentas con plivilegios administrativos utilizan una cuenta nominativa sin privilegios de administrador para las tareas habituales y accesos a Internet o correo electrónico?
- Las cuentas de administración, ¿son nominativas? (es decir, cada usuario tiene la suya propia, no permitiendo el uso compartido de cuentas genéricas)

  En caso contrario, relacionar las cuentas de administración de uso compartido.
- Si existen cuentas de administración de uso compartido, ¿cómo se controla su uso? ¿cómo se gestiona la contraseña (distribución, cambio periódico, cambio tras cese de una de las personas que la conocían, etc.)?

4-4 Mecanismos de autenticación

- Para cada una de los sistemas / tecnologías existentes en la entidad, indicar el mecanismo de autenticación de las cuentas de administración.

  Si se utilizan contraseñas indicar las principales características de la política de autenticación (longitud mínima, vigencia máxima, vigencia mínima, requerimientos de complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales), histórico de contraseñas recordadas).

Sistema / Tecnología	Mecanismo de autenticación	Características principales
Ej: SGBD Oracle 11.2	Contraseña	….
Ej:Aplicación XXXXX	Certificado + contraseña	….
Dominio Windows (servidores y equipos de usuario)	Certificado + contraseña	

- ¿Se dispone de un procedimiento para regular la gestión de las cuentas de administración? (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.)
- El procedimiento anterior ¿contempla el que se retiren/deshabiliten/eliminen las cuentas de administración cuando la persona termina su relación con la entidad?

4-5 Auditoría y control del uso de las cuentas con privilegios de administración

- Se dispone de un registro de actividad de las acciones realizadas con cuentas y sobre cuentas de administración para todos los sistemas (sistemas operativos, bases de datos, aplicaciones, etc.) de la entidad?
- ¿Contempla el registro tanto de acciones exitosas como fallidas?
- ¿Existe algún sistema en el que el registro anterior no esté habilitado? En caso afirmativo, indicar cuál.
- ¿Existen alertas automáticas cuando se asignan/desasignan privilegios de administración? ¿Quién las recibe y las aprueba en su caso?
- ¿Existen alertas automáticas cuando se supera un umbral de intentos de acceso fallidos mediante una cuenta con privilegios de administración?
- ¿Qué mecanismos se utilizan para evitar que los propios administradores de los sistemas modifiquen los registros de auditoría de las acciones realizadas con cuentas de administración?

Documentación necesaria:

- Copia del procedimiento de gestión de privilegios (en particular, privilegios de administración)
- Copia del procedimiento de inventariado de cuentas de administración
- Copia del inventario de cuentas de administración
- Copia del procedimiento de instalación/bastionado de sistemas, o aquél que contemple el control de renombrado/eliminación de cuentas estándar con privilegios de administración y las correspondientes contraseñas
- Copia del procedimiento de gestión de cuentas de administración (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.)
- Copia del procedimiento para el registro de las acciones realizadas con cuentas de administración.

CBCS 5: CONFIGURACIONES SEGURAS DE SOFTWARE Y HARDWARE EN DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES

5-1 Configuración segura

- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación?
- ¿Qué tipo de dispositivos cubre (servidores, equipos de sobremesa, portátiles, móviles y tabletas, etc.)?
- ¿Se utilizan imágenes o plantillas para aplicar la configuración de seguridad de todos los sistemas, de acuerdo con estándares aprobados por la organización?
- ¿Se realizan pruebas de seguridad antes de pasar a producción para comprobar que se cumplen los criterios en materia de seguridad?
- ¿Se dispone de alguna herramienta para realizar la tipología de pruebas anterior? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- Previo a la puesta en servicio de un nuevo sistema, aplicación, etc. ¿se realizan análisis de vulnerabilidades, pruebas de penetración y/o inspecciones de código fuente?

CBCS 5-2: Gestión de la configuración

- Tras la puesta en producción de los sistemas, ¿se realizan comprobaciones periódicas para verificar que la configuración actual no ha sido modificada de forma no autorizada respecto de la configuración de seguridad original?
- ¿Se dispone de alguna herramienta para realizar la tarea anterior? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- ¿Se utilizan herramientas de configuración de los sistemas que impiden la modificación de la configuración de seguridad? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- ¿Se utiliza un sistema de supervisión de configuración para "monitorizar" en tiempo real la configuración de seguridad de todos sistemas de producción de la entidad? ¿La herramienta anterior permite definir alertas cuando se realizan cambios sobre dicha configuración?

  En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- En caso de no disponer de herramientas que impidan o monitoricen la realización de cambios no autorizados en la configuración de seguridad de los sistemas ¿se dispone de otros mecanismos que garanticen lo anteior?

Documentación necesaria:

- Copia del procedimiento de pruebas de seguridad previas al pase a producción (en el que se detalle el alcance (qué sistemas deben pasar estas pruebas), responsables de definir las pruebas, ejecutarlas, aprobarlas, herramientas para realizarlas, etc.).
- Ejemplo del plan de pruebas de seguridad y resultado de su ejecución para un cambio realizado durante el año.
- Copia del procedimiento que regule la realización de análisis de vulnerabilidades, pruebas de penetración y/o inspección de código fuente previo al pase a producción.
- Ejemplo del resultado de un análisis de vulnerabilidades, una prueba de penetración y una inspección de código fuente realizados durante el ejercicio.
- Copia del procedimiento de gestión de la configuración (aquél que indique cómo garantizar que las configuraciones de seguridad no son modificadas de forma no autorizada tras la puesta en producción de un sistema.

CBCS 6: REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (Mantenimiento, monitorización y análisis de los LOG de auditoría)

6-1: Activación de logs de auditoría (registro de la actividad de los usuarios)

- ¿Se registran las actividades de los usuarios en el sistema? En caso afirmativo indicar en qué sistemas (sistema operativo, bases de datos, aplicaciones) se encuentra activada.
- ¿El registro de auditoría indica quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario?
- ¿Se han habilitado las opciones del registro de auditoría para que incluya información detallada, como direcciones de origen, direcciones de destino y otros datos útiles?
- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados?

6-2: Almacenamiento de logs: Retención y protección

- ¿Dónde quedan almacenados los registros de actividad?
- ¿Se dispone de un inventario de los registros de actividad donde además se recoja el personal autorizado a su acceso, modificación o eliminación?
- ¿Qué mecanismos existen para proteger los registros de actividad frente a accesos y modificaciones o eliminación?
- ¿Está determinado el periodo de retención de los registros de actividad?
- ¿Se cuenta con un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención?
- ¿Cómo se asegura que la fecha y hora de los mismos no puede ser manipulada?
- ¿Se realizan copias de seguridad de los registros de actividad?
- ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos?
- ¿Qué mecanismos existen para proteger las copias de seguridad de los registros de actividad frente a accesos y modificaciones o eliminación?

6-3: Centralización y revisión de los registros de la actividad de los usuarios

- ¿Se centralizan los logs generados en los diferentes sistemas?
- ¿Cómo? (volcado diario de los logs, reenvío de los logs al sistema central una vez escritos en el sistema original, escritura directa del log del sistema en el equipo centralizador de logs, etc.).
- ¿Se revisan los registros de actividad en busca de patrones anormales? En caso afirmativo, indicar alcance de las revisiones, responsables de su realización y periodicidad.

CBCS 6-4: Monitorización y correlación

- ¿Se dispone de alguna herramienta/utilidad que permita alertar, en tiempo real de sucesos anormales a partir del análisis de los logs de auditoría?

  En caso afirmativo, indicar nombre de la herramienta fabricante y versión.
- ¿La entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de logs para realizar correlación y análisis de logs?

  En caso afirmativo, indicar nombre de la herramienta fabricante y versión.

Documentación necesaria:

- Copia de la política o normativa que establezca las directrices sobre el registro de actividades de los usuarios (qué se debe registrar, con qué detalle, de qué sistemas, periodo de retención, mecanismos de protección de los registros, etc.).

- Copia del inventario de los registros de actividad, donde además se recoja el personal autorizado a su acceso, modificación o eliminación.
- Copia del procedimiento en el que se establezca:
  - El periodo de retención de los registros de actividad y periodo de retención de evidencias tras un incidente.
  - Proceso para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen).
- Copia de la política de copia de seguridad de los registros de actividad (si se sigue una política específica para este tipo de información, no incluida en la política general de copia de seguridad de datos y sistemas (ver CBCS7)).
- Copia del procedimiento para la centralización de logs, en el que se indique las fuentes origen a centralizar, cómo se realizará la centralización, periodicidad, etc.
- Copia de una revisión de los registros de auditoría realizada durante el año y/o de los resultados obtenidos.

CBCS 7 Copia de seguridad de datos y sistemas

7.1.- Copia de seguridad de datos y sistemas

- ¿Se realizan copias de respaldo que permitan recuperar datos perdidos con una antigüedad determinada?

En cuanto a la política de copia de seguridad:

  - ¿Incluye datos (información de trabajo) de la entidad?
  - ¿Algún sistema, conjunto de datos, etc. queda fuera del alcance de la política de copia?
  - ¿Abarca los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga?
  - Si se utiliza criptografía para el cifrado de la información, ¿la política de copia incluye el respaldo de las claves criptográficas?
  - Indicar tipo de copia y periodicidad (ej. Incremental diaria, completa semanal, etc.).
  - ¿Se dispone de herramienta/s para la realización de copias de seguridad? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
  - ¿En qué soporte se almacenan las copias de seguridad realizadas?
  - ¿Se externalizan las copias de seguridad? ¿Dónde? (ej. a un edificio distinto, a una sala distinta dentro del mismo edificio, a las instalaciones de un proveedor, etc.)
  - Se utilizan servicios en la nube para el almacenamiento de backups? En caso afirmativo, indicar qué servicio se utiliza y el proveedor que lo presta.

7.2.- Pruebas de recuperación

- ¿Se realizan pruebas de recuperación a partir de las copias de respaldo realizadas?
  - Indicar alcance de las pruebas de recuperación y periodicidad.
  - ¿Se documentan (o queda algún registro) de la realización de dichas pruebas de recuperación y las incidencias identificadas?

7.3.- Protección de los backups

- ¿Los backups disfrutan de la misma seguridad que los datos originales, tanto en su acceso, almacenamiento como transporte?

  Indicar brevemente los mecanismos utilizados para dicho propósito.
- En cuanto a solicitudes puntuales de recuperación de datos por parte de los usuarios de la organización, ¿se dispone de un procedimiento que establezca cómo debe realizarse (quién puede solicitar, cómo, quién debe autorizar, etc.)?
- ¿Las copias de seguridad están accesibles de forma directa a nivel de red?
- ¿Se dispone de una copia de seguridad en un soporte desconectado de la red? ¿Cómo y con qué frecuencia se realiza?

Documentación necesaria:

- Copia del procedimiento de copia de seguridad de datos y sistemas
- Copia del procedimiento de restauración a partir de las copias de seguridad realizadas
- Copia de los informes, registros, etc. de las pruebas de recuperación realizadas en el último año
- Copia del procedimiento para la solicitud de recuperaciones puntuales de información a partir de las copias de seguridad realizadas

CLCS 8 CUMPLIMIENTO DE LEGALIDAD

8.1.- Esquema Nacional de Seguridad

- ¿Dispone de una política de seguridad escrita?
- ¿Ha sido aprobada por el órgano superior competente (conforme al Art. 11 del RD 3/2010)?
- ¿Se han asignado los siguientes roles/responsabilidades? En caso afirmativo indicar nombre y puesto de la persona a quien se le ha asignado.
  - Responsable/s de la información
  - Responsable/s del servicio
  - Responsable de la seguridad (STIC)
  - Responsable del sistema (TIC)
- ¿Se ha realizado la auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta? En caso afirmativo, indicar la empresa encargada de la realización de la auditoría.
- Para los sistemas de categoría Básica, ¿se ha realizado la autoevaluación de cumplimiento exigida en el ENS o bien, de forma opcional, la auditoría de cumplimiento?
- Los resultados de la auditoría y de la autoevaluación ¿han sido revisados por el responsable de seguridad y las conclusiones presentadas al responsable del sistema para que adopte las medidas correctoras adecuadas?
- ¿Facilita los datos necesarios para el Informe del Estado de la Seguridad a través de la herramienta INES, cumpliendo así la Instrucción Técnica de Seguridad aprobada por resolución de 7 de octubre de 2016 ?

8.2.- LOPD/RGPD

- ¿Se ha designado Delegado de Protección de Datos (DPD)? En caso afirmativo indicar nombre y puesto de la persona designada, indicando su posición en el organigrama general de la entidad.
- ¿Se ha comunicado su designación a la Agencia Española de Protección de Datos?
- ¿Se dispone de Registro de actividades de tratamiento, de acuerdo a lo establecido en el artículo 30 del RGPD?
- Se han realizado los analisis de riesgo de los tratamientos de datos personales realizados por la entidad y las evaluaciones de impacto para aquellos de riesgo alto?
- ¿Cómo evalúa y verifica la entidad la eficacia de las medidas técnicas y organizativas (ej. mediante auditorías realizadas por empresas externas, autoevaluaciones de cumplimiento, etc.).

8.3.- Ley de Impulso de la factura electrónica y creación del registro contable de facturas

- ¿Se dispone del informe de auditoría anual de sistemas exigido por la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas?

Documentación necesaria:

- Copia de la Política de seguridad requerida por el ENS
- Copia de los registros (ej. resoluciones, actas, etc.) correspondientes a la designación de los responsabes de la información, del servicio, de seguridad y del sistema según el ENS
- Copia de la informe de auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta
- Copia de la autoevaluación de cumplimiento para los sistemas de categoría Básica según ENS
- Copia del documento que recoge los datos de la última declaración en la herramienta INES
- Copia de la designación del Delegado de Protección de Datos
- Copia del registro de actividades de tratamiento de datos de carácter personal

- Copia de los analisis de riesgos y evaluaciones de impacto de los tratamientos de datos personales
- En los casos en los que aplique, copia del informe de auditoría o de la autoevaluación de la eficacia de las medidas de seguridad aplicadas a los datos personales
- Copia del informe de auditoría de sistemas exigido en el Art. 12.3. de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas